LIBRARY > ARTICLE

Managing Risks of the Mobile Enterprise

October 1, 2012 | Abstract of source article authored by ERM Initiative Faculty, 2014 (https://erm.ncsu.edu/library/all-articles)

Mobile devices dominate consumer use to the point that enterprises are seeing the value of integrating them into the workplace as well. This surge in the use of mobile devices within a business enterprise potentially gives rise to various risks that need to be identified and effectively managed to avoid irreversible security and, ultimately, enterprise detriments. In order to ensure that such mishaps are prevented to the best possibility, while maximizing the business opportunities of the mobile enterprise, effective security controls should be implemented to adequately manage the enterprises' risks. A recent paper issued by the Security for Business Innovation Council (SBIC) provides an analysis of the risks along with the recommendations and the valuable insights of nineteen security leaders from large global enterprises.

Factors that define the current mobile trend

- Consumer Behavior Change – The use mobile devices has outgrown other IT used in most workplaces. People are demanding their use more than ever and such consumer changes are propagating the mobile trend. In fact, employees now expect the use of mobile devices.
- Bring Your Own Device (BYOD) – Most people prefer consolidating their personal and work lives together into one phone. Embracing that blend has increased the use of such mobile devices. Furthermore, more than 60 percent of organizations enable "Bring Your Own Device" programs.
- Mobile Computing – Mobile computing has become a core part of the way people interact, communicate, and live their lives. Various apps for normal daily life such as calling cabs, checking the nearest grocery store, hosting parties, finding a theatre nearby is a convenience. Such a powerful trend towards mobile computing has contributed to a surge in the mobile trend.

Benefits of the mobile enterprise

The most important benefit is the flexibility it brings to the work force. It empowers employees with the latest technologies to perform their tasks more efficiently and effectively. The access to corporate information and documents is faster, and hence decisions and communications can be made faster. Furthermore, mobile devices help increase productivity and agility to do a number of tasks in their personal lives and they want to reap those same advantages for their business lives. Enterprises are beginning to empower their customers with the various multitudes of apps to make life more comfortable.

Risks of the mobile enterprise

The risks associated with mobile devices are complex. In order to manage risks, security professionals need to fully understand the risks involved.

1. Lost or Stolen devices – This is perhaps the greatest security concern for most enterprises. Over 80 percent of respondents to the SBIC survey rated this factor as the number one mobile security concern. The volume of intellectual property and proprietary information such as earnings data could get into the wrong hands and adversely impact the company. Various legal risks arise as lost or stolen devices could trigger disclosure breaches. With increasing number of mobile devices, the risk also increases.

1. Mobile Malware – Creating an environment of allowing application access to data and system resources can aggravate this risk. Organizations such as Apple are able to curb malware by employing "application sandboxing" by limiting application access. However, malware developers are always finding different ways to breach devices.

1. Advanced Threats – With sophisticated cyber adversaries and attacks on networks, enterprises need to identify advanced threats in order to prepare or mitigate such a threat. To monitor such threats, organizations use intrusion detection systems (IDS) and other tools to capture potential suspicious activities. However, mobile traffic on carrier networks is almost impossible for enterprises to track.

1. Software Vulnerabilities – Patching or fixing a software problem in the mobile world is more complex than doing so in a PC as different types of updates may be required. This could lead to slower updates that could make the devices vulnerable to attacks. The evolving technologies at the operating system levels may move faster than creating new security controls. Jailbreaking and rooting are two types of schemes to make devices fully vulnerable to outside attacks. Sometimes, users may be unaware that their devices are jailbroken.

1. End-user Behavior – This pertains to users being complacent and not being careful about the way they use their devices. Using the cloud-based storage for corporate data represents a significant risk. Various apps could be collecting user information from the device. Hence, users can unintentionally download an app that contains crimeware, which could be stealing sensitive files and corporate data. Allowing employees to use their personal mobile devices can also be detrimental since enterprises will have less control over end-user behavior.

1. Compliance and Legal Issues – Integrating personal and professional data on one device can create difficulties in managing business risk and protecting users' privacy. Enterprises must understand the risks they assume with BYOD since privacy laws do not allow an enterprise to legally wipe the device when an employee leaves the company. So many legal and compliance issues can arise as a result.

Recommendations for Managing Risks of the Mobile Enterprise

1. Establish mobile governance – To successfully manage the risks of mobile devices within an enterprise, organizations must create policies and processes, integrate security into mobile plans, and educate/train its end users. This is referred to as mobile risk management, and it will not be effective if it is treated in a siloed fashion. Stakeholders must establish policies and processes that are cross functional to the fabric of the organization. Collaboration of security and IT with all business units such as operation, legal, human resources, finance, accounting, and compliance is imperative to make this effective.

1. Create an action plan for the near term – Mobile devices change constantly. However, it is recommended to create an action plan to effectively manage risks for the near term while having a vision for the long term. Some of the guidelines for the near term include:

    A Master Data Management (MDM) solution that can help and secure consumer mobile devices. This solution can serve as an interim solution and not an effective long term strategy.

    Containerization can help protect sensitive enterprise data on BYOD programs that integrate work/personal devices.

1. Build core competencies in mobile app security – This is a keystone of mobile risk management where mobile apps should have enterprise-grade security capabilities. Organizations should also employ best practices in mobile application security that includes various security features. Furthermore, organizations must keep in mind that the real business value of going mobile should be assessed and weighed against the cost and security factor rather than by the coolness factor.

1. Integrate mobility into long-term vision – Mobile computing is an integral part of many organizations. Hence, it is imperative to view its integration into the long term strategies that can manage and resolve various risks identified above. Traditional enterprise boundaries are almost non-existent now, and security teams must be agile and fast in detecting, understanding and managing such risks to propagate the organization's long term strategies.

1. Expand mobile situational awareness – Organizations must invest in educating and training its employees in a comprehensive understanding of the mobile space. Furthermore, corporate security teams must dive deeper into the factors that affect mobile risk management and consider how such risks affect the overall enterprise risk management.

Financial motivations can entice attackers to devise complex and sophisticated methods to exploit the mobile space and do irreversible damage. It is crucial to also understand how to effectively implement the mobile risk management as its effectiveness will directly affect the overall enterprise risk management. Hence, it is critical to develop the tools, knowledge and foresight necessary to counter such mobile threats and preserve and potentially increase the value of the mobile enterprise.

Link: EMC Corporation (http://www.emc.com/collateral/industry-overview/h11109-rsa-realizing-mobile-enterprise.pdf)

Topics: Miscellaneous ERM Topics (https://erm.ncsu.edu/library/categories/category/miscellaneous-erm-topics),
Interaction of ERM and Strategic Planning (https://erm.ncsu.edu/library/categories/category/interaction-of-erm-and-strategic-planning),
Risk Management Fundamentals (https://erm.ncsu.edu/library/categories/category/risk-management-fundamental),
Risk Management Tools and Techniques (https://erm.ncsu.edu/library/categories/category/risk-management-tools-and-techniques),
ERM and Strategy (https://erm.ncsu.edu/library/categories/category/erm-and-strategy),
Risk Management Strategies (https://erm.ncsu.edu/library/categories/category/risk-management-strategies)

SHARE

34

BROWSE TOPICS

View All Topics(

View All Articles(

ERM Library Topics 624

Browse All Topics

NC STATE

Enterprise Risk Management Initiative

Poole College of Management, NC State
2801 Founders Drive
Campus Box 8113
Raleigh, NC 27695

Quick Links

- About ERM Initiative (https://erm.ncsu.edu/about-erm/)
- Advisory Board (https://erm.ncsu.edu/about-erm/advisory-board/)
- ERM Article Library (https://erm.ncsu.edu/library)
- Executive Training (https://erm.ncsu.edu/executive-education)
- Courses (https://erm.ncsu.edu/courses)
- ERM Experts (https://erm.ncsu.edu/smes)
- Contact ERM (https://erm.ncsu.edu/about-erm/contact-erm/)

ERM Initiative @ NC State

(https://www.google.com/maps/place/Enterprise+Risk+Management+Initiative+ERM/@35.788656,-78.673886,15z/data=!4m5!3m4!1s0x0:0xed2c011c06a18082!8m2!3d35.788 78.673886)