Managing risk in mobile commerce

Patrick L. Brockett*
Department of Information, Risk, and Operations Management, McCombs School of Business, University of Texas at Austin, Austin, Texas 78712, USA
Fax: (512)-471-0587
E-mail: brockett@mail.utexas.edu
*Corresponding author

Linda L. Golden
Department of Marketing, McCombs School of Business, University of Texas at Austin, Austin, Texas 78712, USA
Fax: (512)-471-1034
E-mail: UTlindagolden@gmail.com

Anji Song
Department of Accounting, McCombs School of Business, University of Texas at Austin, Austin, Texas 78712, USA and PricewaterhouseCoopers, 488 Almaden Boulevard, Suite 1800, San Jose, California 95110, USA
E-mail: anji.song@us.pwc.com

Abstract: Mobile commerce (m-commerce) is an increasingly important component of the consumer and business marketplace which, according to ABI Research, is expected to grow to $119 billion in 2015. With the large number of users and the prevalence of smart phones, m-commerce presents an opportunity for businesses to expand their market (and the potential threat to lose market share if they do not participate). Along with m-commerce opportunities, however, comes risk. In the rush to present an m-commerce face to the mobile consumer, risks are engendered and vulnerabilities uncovered that could threaten the enterprise and peril the consumer. Here, we discuss the growth of m-commerce as it affects the risk of the corporation and consumer. We also discuss steps that can be taken to mitigate and finance m-commerce risks for firms and individuals.
Keywords: mobile commerce; m-commerce; risk management; e-business; e-commerce; wireless vulnerabilities; risk identification.


Biographical notes: Patrick L. Brockett is the Gus Wortham Chairholder in Risk Management, University of Texas-Austin McCombs School of Business, with appointments in information, risk and operations management, finance, and mathematics. He received his PhD in Mathematics from the University of California at Irvine. He is a Fellow of the Institute of Mathematical Statistics, the American Statistical Association, The Institute of Risk Management, and the American Association for the Advancement of Science. He directs the Center for Risk Management and previously directed the Center for Cybernetic Studies at the University of Texas. He has published in a variety of journals including Management Science, IEEE Transactions on Information Theory, Journal of Risk and Insurance, Journal of Marketing Research, Annals of Statistics, and others, and his articles have won several awards.

Linda L. Golden is a Professor of Marketing and Marlene and Morton Meyerson Professor in Business, University of Texas at Austin. She received her PhD from the University of Florida and her JD from the University of Texas-Austin. She has published in attribution theory, comparative advertising, retail image and patronage behaviour, social marketing, risk management, and efficiency analysis of business. Her research on predicting insolvency won the American Risk and Insurance Association Award for that article with a lasting ten-year impact on risk management. Both her fraud prediction research and her work on social and psychological influences on consumer financial risk taking received the Casualty Actuarial Society Award (in 2002 and 2008 respectively) for having the greatest impact on casualty actuarial science. She has published in Journal of Consumer Research, Journal of Marketing Research, Management Science, Journal of Mathematical Sociology, Journal of Risk and Insurance, and Multivariate Behavioral Research.

Anji Song graduated in 2011 with a Masters in Professional Accounting from the McCombs School of Business at the University of Texas at Austin where, in 2010, she worked as a Graduate Teaching Assistant. After graduation she joined the assurance group at PricewaterhouseCoopers in San Jose where she holds the position of Assurance Associate.

1 Introduction

Mobile commerce (m-commerce) is growing in importance. Indeed, according to the Experian Marketing Services annual 2010 Holiday Marketer Benchmark Trend Report (quoted in Schwartz, 2010), 22% of consumers used their phones to check prices, 21% researched about products, and 13% of consumers with web-enabled phones made purchases with their mobile phones. Compared with 2009, consumers were 38% more likely to find mobile ads from businesses including sales or promotions useful (Schwartz, 2010). The percentage of the advertising budget devoted to mobile advertising by firms is expected to grow from 0.5% of the total advertising budget in 2010 to 4% of the budget by 2015, and worldwide the revenue from mobile advertising is projected to reach
Managing risk in mobile commerce

$3.3 billion in 2011 (Gartner, 2011). Mobile retailing is, together with many other wireless business activities, giving rise to yet another revolution in the business world, this one centred around conducting business on the move – so called mobile commerce and abbreviated as m-commerce (Coursaris and Hassanein, 2002). Fuelling this growth is the rapid expansion of mobile phones and smart phones in particular. Smartphone sales were up 49% in the first quarter of 2010, achieving 54 million sold (BBC News Technology, 2010; quoting a research study by Gartner Group). According to a study by the National Retail Federation 74% of online retailers either have an m-commerce strategy in place or are developing one (Marcus, 22 July 2010). Among retailers not already engaged in m-commerce, one quarter say that they intend to begin within the next year (Siwicki, 2010). An early assessment and overview of mobile commerce marketing opportunities can be found in Balasubraman et al. (2002).

Wireless communication networks provide the backbone for m-commerce activities, transmitting data between mobile devices (such as phones or iPads) and other computing devices such as retail store or office computers. Although wireless networks were introduced in 1946, it was the introduction of the advanced mobile phone system (AMPS) in 1983 that marked the arrival of a cellular communication system in the USA (Coursaris and Hassanein, 2002). M-commerce ultimately became a natural extension of e-commerce, as they share fundamental business principles. However, m-commerce acts through a different communication channel that adds value, reach, and convenience to the e-business processes. This different communication channel, however, also exposes the enterprise (and consumers using it) to different and additional risks necessitating different risk management techniques.

While the m-commerce and the e-commerce business environments and activities have a lot in common, it is imperative to make distinctions between the two to develop a more precise understanding of m-commerce, its applications, and the unique challenges and especially the risks associated with this new business model. M-commerce differs from e-commerce in the mode of communication, the types of internet access devices, the development languages, and communication protocols, as well as the technologies used to enable and support each environment (Coursaris and Hassanein, 2002). This paper will discuss these risks and possible risk mitigation techniques appropriate for companies entering this new and growing retail market.

2 Risks associated with mobile commerce

Friedman et al. (2011) point out that the risk differences between traditional e-commerce modes and wireless m-commerce can be largely attributed to the different communication platforms used to access the company’s computers. Discussing the difference in the physical characteristics of their cyber risk and how those threats affect users they note:

“When communicating via a wireline, it is intuitive to most that the data traffic is leaving the computer through a data cord to an interface that connects with the Internet Service Provider. … It is quite difficult for a typical cyber criminal to intercept data on a … cable that he had not physically tapped. The same cannot be said of wireless network communications. Malicious actors can learn a great deal from unencrypted Wi-Fi links in their vicinity. … [I]f the wireless connection is not itself encrypted using a modern standard (i.e. WPA2), then any nearby attacker can listen to all unencrypted traffic traveling between the computer and the wireless router. The data are being broadcast to the
surrounding area by both the computer and the router in the same way that noise from a conversation is vulnerable to eavesdroppers. Thus, information can be intercepted. Tools to capture this traffic and reassemble the data packets into web pages are widely available, and usable to any moderately sophisticated computer user.” [Friedman et al., (2011), pp.4–5]

Fraud risk is an example of an already existing risk which may be amplified by using mobile networks. According to the 2nd Annual True Cost of Fraud Study, conducted by LexisNexis Risk Solutions and Javelin Strategy and Research and quoted in Siwicki (2010), the risk of fraud faced by web-only merchants is 0.83% of transactions and for multichannel merchants with both an e-commerce site and physical store locations this percentage is 0.86%. For multichannel merchants with an e-commerce site, stores, and an m-commerce site or application the percentage grows to 1.13%. While these merchants differ in respects other than simply their use of m-commerce, it suggests that when merchants open up new transaction channels, they raise the possibility of opening up new fraud opportunities. Mobile entry into the shopping portal arena exposes vulnerabilities of companies not present in physical shopping or in e-commerce using cables or land lines, namely, intercepted transmissions of information and passwords.

Web owners and companies conducting business over the internet and through mobile devices have to protect themselves from four major operational risk exposures related to:

- technical: network/software and hardware deficiencies
- legal: non-compliance/lawsuits
- physical security: unauthorised access/business continuity risks
- privacy risks.

The above operational risks may lead to broader category risks such as financial risks and privacy risks and eventually evolve into reputational risks and strategic risks that threaten the very existence of the business.

### 2.1 Technical risks

To access the internet from a mobile device, a wireless application protocol (WAP) or another competing protocol must be used to effect the transmission. Such connections, if not properly executed, can be faulty, dropped, or subject to hijacking or eavesdropping causing legal risks of a greater magnitude than that experienced in ordinary hardwired PC connections. An inherent concern about mobile network usage is that loss of connection can result in loss of data (Gillick and Vanderhof, 2000). This loss of data can yield anything from a simple interruption of web surfing to loss of critical information used in financial transactions. The cost for unreliable connections could be high, as it would encompass business losses and legal charges including fees and fines (Coursaris and Hassanein, 2002), and of course, lost sales.

An accompanying risk is that most receiving websites are not configured to handle high frequency momentary interruptions in connectivity which are more common in m-commerce than e-commerce (Ghosh and Swaminatha, 2001). Additionally, reinstatement of the interrupted connection is often done without re-authenticating the user, thus allowing an opening for a criminal to hijack the transmission and access records or enter into the firm’s internal IT system. This access can later be used for
Managing risk in mobile commerce

171

malicious purposes (Ghosh and Swaminatha, 2001). A criminal, by simply refreshing the accessed website also may gain malicious entry into the company’s computer system or the individual consumer’s bank account. The threat is not insignificant. Indeed, according to data released by ComScore, 13.2 million people accessed their bank accounts from their phones during the month of April 2010, a 70% increase from the previous year. And similarly, the number of people using mobile banking applications more than doubled, to approximately 5 million in 2010 (quoted in Marcus 22 July 2010).

The platform or operating system that businesses use provides the basic infrastructure for running m-commerce applications. Without a secure infrastructure for computing on the hosting device, achieving secure m-commerce may not be possible. The platforms and languages being developed for wireless devices have sometimes failed to utilise basic security concepts present in today’s desktop machines (Ghosh and Swaminatha, 2001).

While the operating system provides the basic platform for wireless applications, the software applications that run on the mobile devices themselves are equally important. Flaws in the logic and implementation internal to the mobile device can result in security loopholes and be exploitable by attackers or malevolent websites. Moreover, typically the languages used for development in handheld devices are not as sophisticated (for space and speed rationales) and unless corrected, this will ensure the continuation of basic flaws. The physical limitations (size, memory, non-functional requirements such as necessity of illuminated screens, limited power, processing cycles, bandwidth, etc.) of a mobile device often force application developers to make security versus performance trade-offs. These limitations can, for example, force application developers to give up security features such as encryption in an effort to improve online performance (Ghosh and Swaminatha, 2001). Even in the presence of encrypted communication, great risk exists because of the false sense of security encryption provides to end users. Also, malicious codes penetrating wireless networks and accessing the mobile device have the ability to render other security features such as authentication and encryption ineffective. This is achieved through the ability of the malicious code to run while residing on the device with all the privileges of the owner (Ghosh and Swaminatha, 2001).

As with any form of commercial exchange, m-commerce involves multiple steps, including search, information exchange, negotiation, contracting, delivery and settlement. For m-commerce, the settlement step necessitates considerably greater care than the others, not only because the payment process creates considerable opportunities for funds to be stolen, but also because of the fact that mobile settlement relies strongly on virtual technologies, which are more prone to hacking and unexpected attacks. Compared with the physical transfer of funds in regular face-to-face commerce, a thief penetrating the technical end of a mobile transaction is unlikely to be apprehended, and it will be almost impossible to recover the proceeds. The victim may not even be aware that the theft has occurred (Clarke, 2008).

From the perspective of the consumer, the m-commerce end user faces similar technical risks to the m-commerce service providers, namely unreliable business network, malfunctioning of merchant’s software application or hardware breakdown of mobile devices. The consequences however, may be different. Such technical risks may cause customers inconvenience (resulting in their moving to another site for purchases), but could also precipitate a loss of personal funds and private information if technical deficiencies are exploited for illegal purposes (e.g., identity theft, emptying bank accounts, phishing attempts, etc). While some of these risks are mitigated for individual consumers (the bank must reimburse the individual for money illegally taken from their
accounts) this reimbursement is not required for commercial and non-profit enterprises who do not have the same legal protection against cyber thievery of bank accounts using the internet (Johnson, 2011). Thus, security risk is critical for both ends of the communication chain.

2.2 Legal risks

The financial institution’s legal obligation, once the customer’s order is received, is to complete each financial transaction initiated by the customer. Financial institutions under the Federal Trade Commission’s jurisdiction are required to ensure the security and confidentiality of personal information collected from their customers. Financial institutions are legally responsible to maintain security within their information systems, including network and software design, information processing, storage, transmission, retrieval, and disposal. As illustrated previously regarding theft from bank accounts of individual consumers, financial institutions are subject to a wide array of federal, and to a lesser extent, state laws and regulations governing the way in which they handle customer information (e.g., mobile payments may also be subject to wire transfer laws and regulations). Wireless carriers, on the other hand, are by law deemed to be ‘limited liability’ entities. They have no affirmative legal obligation at this time to do anything except to ensure that a voice or data communication is originated and terminated, and to refund the calling party for the cost of that transmission if the communication fails. As the volume of mobile banking and mobile finance traffic increases, the tension inherent in this risk allocation (wireless carriers or mobile internet device manufacturers creating vulnerabilities, but banks regulated to do reimbursement) is likely to grow. Financial institutions will undoubtedly be interested in seeing that these risks are shared in ways not currently required by law (CTIA – The Wireless Association, 2009). Economic theory suggests that the most efficient allocation of risk costs is to have the entity most able to control loss costs be most responsible for loss payments, so a move toward shared or reallocated risk costs is economically warranted.

From the consumer perspective, the legal risks and remedial rights available for disputing unauthorised transactions and incorrect charges may differ depending on how payment is made. In addition, although banks may reimburse for account thievery, consumers may not be protected from their mobile service being terminated for failure to pay disputed charges that were billed to their mobile accounts by hijackers or hackers. They may also find it hard to prove the terms on which they purchased items on their mobile devices if the details of transactions are not confirmed (e.g., on itemised phone bills).

Mobile commerce creates other potential legal liabilities for enterprises engaging in wireless transactions because the telephone system has historically been heavily regulated, and smart phones using the telephone system to access the internet must satisfy these telecommunication regulations as well. This is a departure for ordinary hardwired internet commerce. Advertisers using SMS messages or voice messages, for example, can be subject to ‘do not call’ provisions and other telephone legal limitations enabling the consumer to ‘opt out’ of receiving messages. Additionally, the ability of companies to track the location of individuals through the built-in GPS in their smart phone raises legal issues of privacy and informed consent depending on how the enterprise intends to use the data. Many individuals do not want their movements tracked and have legal recourse if clear, informed consent is not obtained prior to gathering. While the ability to
specifically target market to nearby customers or to send coupons to shoppers in the vicinity can be productive (traditional paper coupons have a redemption rate of about 0.2% to 2%, while mobile coupon redemption rates can exceed 50%). According to Tsirulnik (2010), there are legal issues that can arise if not done properly. Mobile payments may also be subject to wire transfer laws and regulations.

Another yet unresolved issue (also present in e-commerce using a hardwired PC, but is exacerbated in m-commerce) concerns the application of international laws and who has jurisdiction to bring a criminal to justice in their court. The ‘long arm’ statutes that allow one jurisdiction to bring someone from another jurisdiction to trial in their venue are unclear with respect to m-commerce crimes. For example, whose laws and jurisdiction apply when an American consumer travelling in England uses their smart phone on an English wireless network to purchase a product from a French company whose website is served in Germany? Liability issues such as these can be contractually formalised in the initial contracting, but legal vagaries still remain and the enterprise needs to be cognisant of these.

2.3 Physical security risks

Physical security describes measures that are designed to deny access to unauthorised personnel from physically accessing a building, facility, resource, or store of information. In the world of mobile commerce, companies usually are aware of physical intrusion risk and take security steps to safeguard their computers and servers from unauthorised physical access (and buy insurance against physical loss or damage of equipment). However, the enormous volume and the sensitive nature of the mobile transaction information (including the time and location history of the smart phone user) never fail to invite potential compromises of existing security controls from both internal and external attacks.

This possibility has been realised at even the most secure computer systems, the US military computer system. Recently, declassified documents show that a foreign intelligence agency dropped an infected thumb drive in the parking lot of a US Department of Defense facility in the Middle East in 2008. The person finding it put it in their computer (perhaps a natural response to see what was on it or to try to identify the owner) and their computer was connected to the US Central Command. As Deputy Defense Secretary William J. Lynn wrote in Foreign Affairs, the malware spread “undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control” (Flatley, 2010). Similar physical intrusions are easily possible in corporate computer systems, which have lesser degrees of security and less security training for their employees. Physical intrusions by employees (using thumb drives, iPads or other devices) are also a threat to companies handling private, sensitive, or valuable information. In addition, unexpected physical incidents such as earthquakes, floods, or robberies can potentially catch businesses off-guard, disrupting day-to-day m-commerce operations and casting a heavy cloud over business continuity.

From the perspective of the consumer, the risk vulnerability of using m-commerce is enhanced tremendously by mobile devices being physically lost or stolen. Without physical perimeter security, mobile computing devices are at increased risk of theft and loss, particularly given their small size. Studies show that 52% of users store passwords on their phones; and 87.5 million users conduct banking using their phones so huge
losses can result from identity theft if their mobile devices fall into the wrong hands (Siciliano, 2011a). And, according to Siciliano (2011b) two million mobile phones are stolen or lost every year (one every 15 seconds). Most users do not use PIN codes to lock their cell phones, and most consumers use the same password for multiple m-commerce, banking and other sites, thus enhancing the possible risk severity to both the consumer and the company (perhaps employer) if a cell phone ends up in criminal hands, and thus yields entrance into the computer systems with a verified password. Indeed, due to some security problems with the manufacture of some Android smart phones, even the use of a password protection by a customer on their phone can be easily be defeated (Sacco, 2011). Once a password has been obtained, spear phishing (or hacking other websites or the mobile phone itself) may yield other accounts that can be accessed with this same password.

While the data stored on a misplaced device might be irreplaceable or proprietary, other risks of lost internet-enabled devices include the ability for finders of lost devices to access proprietary corporate systems, including e-mail servers and file systems. One of the key problems with the current generation of handheld devices is the lack of good mechanisms to authenticate a particular user to a particular device (Ghosh and Swaminatha, 2001). Unauthorised accesses using mobile devices leads to foreseeable problems such as loss of client data and other confidential business information. Security for mobile devices has not kept up with the technology for cracking into them. Biometric technology (e.g., full face scans, fingerprints and even retinal scans) has proven useful for authentication in hardwired computer systems. Siemens, for example, has already developed fingerprint scanning technology for electronic banking use (Budworth, 2009). However, to date the use of biometric technology in mobile security has not been implemented.

2.4 Privacy risks

From the perspective of a customer, privacy-risks tops the list of their concerns when engaging in mobile transactions. While m-commerce brings about ease and convenience, m-commerce applications introduce new and significant privacy risks to end users. The public is becoming increasingly aware that major marketing and data collection firms such as DoubleClick and Engage are tracking users’ online web usage via cookies with unique identifiers (Ghosh and Swaminatha, 2001). In the wireless web, there will certainly still be tracking of web usage and even more profiling is possible, including time, date and location profiling. Identify theft, where the perpetrator assumes another’s identity in order to access resources or obtain credit and other benefits in that person’s name, has drawn a considerable amount of attention as e-commerce grows. Mobile devices are providing even greater opportunities for data breaches and identity theft, which could lead to substantial personal loss. As an example, according to Sacco (2011) a recent HTC software update for a collection of commonly used smart phones installed an application to collect user information such as “account information (e-mail address, data sync status, etc.); GPS- and network-based locations and a short history of last-visited locations; phone numbers from users’ phone logs; SMS data; and system logs, which could provide information on active apps, e-mail info, phone numbers and other sensitive data”. In addition, this newly installed data logging tool which came with the software upgrade also is reported to allow access to this same data by any other application that the
Managing risk in mobile commerce

user has granted internet access to. This could be a tremendous threat to privacy giving information useful for identity theft.

Additionally, as noted by Ghosh and Swaminatha (2001), in a mobile communication era the person wanting to steal information by hacking a mobile devise no longer needs to pursue their prey. They can simply wait in a wireless location for their prey to come to them or roam through multiple wireless locations, such as airports. An example of such a possibility goes by the picturesque name, Bluesnarfing. It exploits a security flaw in Bluetooth technology that allows users to access and copy information stored on any wireless device using Bluetooth. It is easy to gain access to important data such as contacts, e-mails, pictures, and even videos because the data is usually intercepted between phones, laptops, desktops, and PDAs (Walsh, n.d.). This was demonstrated during the Academy Awards in 2005 by a security consulting firm called Flexilis who positioned themselves in a crowd watching celebrities arrive. They were able to detect that approximately 50 to 100 guests had smart phones, whose contents could be electronically stolen (they did not actually tap any of these phones for legal reasons). They did this to raise awareness of a threat that is becoming more common as cell phones are carrying a growing range of personal data, including passwords, Social Security numbers and credit card information (Markoff and Holson, 2005). Another very publicised example of hacking into phones for nefarious purposes occurred in England where Rupert Murdoch’s international News Corporation’s paper News of the World hacked into the voice mail of such well protected people as members of the Royal Family as well as allegedly hacking into the phones of a murdered English schoolgirl, relatives of British soldiers who had died, and even some of the victims of the terrorist bombings in London on 7/7/2005. According to BBC News (2011), the police are contacting people on a list of approximately 4,000 people who may have been hacked, including celebrities, politicians, and sports stars.

The benefit of being reached anywhere anytime poses significant privacy risks to users as they become victims of SMS spam, voice messages, telemarketing and more intrusive marketing (Datamonitor, 2001). Location-oriented marketing services also could lead to other uses of information about consumers’ activities and locations that they neither expected nor desired. Important personal information given to vendors to make mobile commerce transactions could be intercepted in transmission or obtained surreptitiously by hidden RFID readers making mobile users and their personal belongings more susceptible to attacks.

2.5 Spear phishing and pharming

Two techniques of stealing information, which can affect both commercial enterprises and individuals and contribute to identity theft and unauthorised access to company computers go by the colourful names of spear phishing and pharming. While both have their origins in the hard wired internet era, they are more pronounced and pose greater risks in the blossoming wireless communication world. Phishing is the old technique of sending multiple (maybe millions or billions) of unsolicited e-mails to individuals claiming to be an official source and asking for personal information ‘for verification purposes’. The phishing expedition masquerades as a legitimate request using hijacked organisation letterhead and logo. They ask the recipient to click on a link to supply information (account number, password, social security number, etc.) in order to verify some aspect of their account. The link and the e-mail are both phony, but if an
unknowing recipient enters personal information, it is captured. Once obtained from the victim, the supplied information (account numbers, PINs, etc.) is used to commit crimes, usually identity theft, unauthorised withdrawals from accounts, or charges on credit cards. Access to secure corporate sites is possible this way as well. Most e-mail users are now alert to this traditional phishing threat and the phishing yield has decreased substantially, leading to the further development of spear phishing and pharming.

2.5.1 Spear phishing

Spear phishing is a refinement which is even more difficult counter. Using some inside information gathered by other means (e.g., hacking a corporation’s computer, social media sites, hacked cell phone, etc.) the criminal, instead of randomly sending out e-mails, does a more selective, controlled and targeted phishing expedition. Using information particularly relevant to this well-defined smaller group of people, they construct an e-mail that is specific and detailed, and contains information making the request credible. Spear Phishing has an enhanced air of being a legitimate request by including the name of a supervisor or trusted superior (obtained from a stolen organisational chart, for example) to solicit the information. Compliance is enhanced by these techniques. Again, if any one of the many targeted individuals within the company responds and logs on, security is breached and computer programmes can be downloaded that allow full access to company computers for espionage purposes, identity theft, and malicious destruction of data, extortion, or financial thievery (FBI, 2009).

2.5.2 Pharming

Pharming is the name given to a different type of hacking technique used to direct the unsuspecting victim to a malicious website where malware can be downloaded or password and account numbers can be harvested in bulk numbers. Unlike phishing where the individual phishing lines (e-mails) are set out to catch fish, in pharming a network node is hijacked and all traffic going through this node is harvested simultaneously. The redirection of the web request occurs at the server level and does not require any compliance by the victim. It is an outgrowth of the older techniques for hardwired PCs known as domain name system (DNS) poisoning, but in a mobile wireless communication world the threat is becoming more prevalent.

This is how it works. Website addresses are a sequence of numbers representing the site. For example, when you type http://www.ABCCompany.com in your browser, the software recognises it as 123.456.7.8. There is a translation mechanism (like a dictionary) built into DNS servers that receives your input and converts the words http://www.ABCCompany.com into the unique numeric website address. A pharmer hacks into the DNS server and changes the translation book or dictionary so that when you (or anyone else using this server) type in http://www.ABCCompany.com, it automatically sends the communication to another site (say 987.654.3.2) instead of the real site (123.456.7.8). Since the phony site looks the same as the original, the unsuspecting user logs in as usual and their account information and password are obtained by the criminal. Malware can be downloaded onto the requesting computer compromising many business activities and trade secrets (Norton, 2011).

Companies involved in internet commerce have major concerns with pharming and the consequent fraud as their clients get scammed. Online banking sites are particularity
Managing risk in mobile commerce

sensitive to this threat. Moreover, adware and spyware removal software and antivirus software is ineffective in protecting against this threat since the hijacking occurs on the DNS server away from the requesting or responding computers, and hence is not detected by either side of the transaction that was hijacked. With the growth of wireless routers (both in businesses and homes) and wide spread availability of free public access Wi-Fi, the potential to hijack data and transactions in mass quantities via pharming a wireless router is an increasing threat that requires very specific anti-pharming defences by the enterprises involved. For example, many home and small business wireless routers come with set of standard authentication pass codes built-in to ID protect them, however most users do not change these passwords and use the default factory password, which hackers can often easily discern to hack into the wireless router (so-called drive by pharming).

Banks and other firms are now employing security firms to construct more sophisticated ways to check their routers and servers to ensure they have not been hacked (e.g., comparing the ‘dictionary’ entries of the selected server with those of three other independent servers to see if there is a difference, or checking the dictionary of the server against a previous copy of itself to see if there has been a rewrite of the server dictionary), but this needs to be an ongoing active process in the mobile communications era.

3 Risk management for mobile commerce

First and foremost, management should identify and assess the risks associated with conducting business through mobile channels through a systematic scoring or rating system based on risk likelihood and risk impact. The resultant risk map will allow management to respond to the risks in one of the four ways detailed below or use a blend of several provided that it is cost-beneficial to do so. Responses include risk avoidance, reduction, sharing, and acceptance. Whichever response management chooses, the goal is to bring residual risk within the firm’s desired risk tolerances.

3.1 Risk acceptance

Management can choose to take no actions to affect the likelihood or impact of current level of risks associated with m-commerce if it is more cost-beneficial to spend valuable firm resources on deploying other opportunities or addressing other risks. This can be a very dangerous and is a potentially costly gamble, but one that is often taken by small firms perhaps ignorant regarding the risks, or simply having an ‘it cannot happen here’ attitude. Additionally, risk acceptance is often the result of insufficient preliminary investigation whereby the risk is retained simply because it was overlooked or not identified with respect to its frequency or severity. This is ‘passive risk retention’ and can be most detrimental since the magnitude of the retained risk has not been examined.

3.2 Risk avoidance

Management may decide to exit or divest their m-commerce activities that are exposing the business to an unacceptable level of risk because it is not cost-beneficial to adopt risk mitigation methods to control. Avoiding m-commerce risk entirely would entail the resulting loss of market presence and has financial consequences, which could ultimately
be as costly in the long run as participating in m-commerce. Certain retail activities may still have the option to exist in an only brick and mortar setting, but most of these will find it necessary to have a web presence, even if no financial transactions are taking place. These businesses can have a web (and mobile web) presence but no purchasing ability over the web, just in the physical stores. Restaurants and other service oriented businesses (e.g., automobile repair shops) can avoid having credit card sales online.

3.3 Risk sharing

There are several ways in which the risk of m-commerce can be shared with others, including contractual sharing with partners and sharing risk contractually with insurers. We discuss these next.

3.3.1 Mitigating the risks via contractual solutions

If data is compromised, there is often no definitive answer as to who is responsible, and ultimately it will depend upon the contracts in place between the m-commerce company and its various partners: application developer, network provider, payment processor and other companies involved with the business. Much of this comes down to the contracts, and if it is not contractually shifted or shared with the partners, it resides with the company itself. Lawyers spend a lot of time trying to allocate risk responsibility in commercial agreements. The premise is that the business will be held responsible unless that responsibility has been transferred to somebody else through contract and service agreements. Outsourced services with powerful fraud prevention features built into them provide merchants with another alternative. Both methods will effectively limit and reduce an entity’s legal (product liability) risks. Examining the partner’s insurance contracts (or even being listed as an ‘other insured’ on their insurance) may be necessary to ascertain if the risk sharing is credible. Periodic auditing of the cyber partners and providers (and their subcontractors who are given access to the corporate IT network) is a necessary component of having an effective risk transfer control mechanism.

3.3.2 Mitigating financial/business interruption and reputational risks by purchasing insurance policies

Commercial general liability (CGL) insurance provides broad general liability for businesses but may not extend coverage if someone’s computer was exposed to a virus on the merchant’s site, or whose confidential information was mishandled (professional liability). Professional liability coverage may come as part of the CGL policy or the company may need to purchase it separately (Baranoff et al., 2009).

A useful insurance coverage in the context of m-commerce risk is business loss or business interruption insurance. This will offer protection to insured businesses who experience shut downs or the inability to generate revenue as a result of unforeseen events, which may include electronic causation.

Insurance coverage against defamation/libel and/or coverage for infringement of copyright or trademark can be purchased for merchants who provide content-oriented web services and are concerned about potential liabilities. Protection for these companies will be provided against allegations of defamation, libel, slander, infringement and invasion of privacy that arise from content published on the web or through mobile

P.L. Brockett et al.
Managing risk in mobile commerce

Another potential policy useful for m-commerce exposed firms is e-commerce insurance (Baranoff et al., 2009). When available, this insurance coverage can involve both first party and third party coverage for potential damages from internet-related activities. Vendors of e-commerce insurance include Chubb’s Cyber Security, Lloyd’s e-comprehensive, and Marsh’s NetSecure. Many insurance companies however, are reluctant to underwrite large amounts of damages due to the relative newness of this specific type of risk, the degree to which the insured has control over the frequency and severity of losses (moral hazard and adverse selection), and the lack of well verified loss data upon which to derive actuarial estimates. Still, Lloyd’s of London offers a $50,000,000 limit under its e-comprehensive policy and can write a custom policy for up to $200,000,000 (Gordon et al., 2003).

As more actuarial and damages data become available and cyber risk protection protocols become more standardised, it is likely that firms will be able to compete more broadly on coverage and premiums. An example policy is AIGs netAdvantage Pro which provides insurance coverage for companies that provide traditional products and services via the internet, or companies that service e-clients. Coverage is offered for claims arising from acts, errors and omissions in the insured’s computer and internet services. This coverage will effectively reduce the impact of physical security risks on businesses.

A further useful example is Allied Assurance Company’s Tech 404v2 webpage which offers a loss calculator which estimates generally the cost that might be expected to arise for a given number of records stolen in a security breach (Allied, 2011) based on the cost of internal investigations, notification and crisis management costs and regulatory and compliance costs. For example, using this calculator, the estimated loss costs for a breach resulting in the loss of 100,000 records would produce a total loss cost of $11,639,040 with $972,720 going to internal investigations attorney fees and cyber crime consulting, $1,942,920 for notification and crisis management including customer notification call centres, crisis management consulting and media management, and $8,723,400 going to regulatory and compliance costs including credit monitoring for affected customers, defence costs of regulatory actions and state and federal fines. This illustrates the magnitude of the potential losses and why insurance is necessary.

3.4 Risk reduction

Actions can and should be taken to reduce the likelihood or impact of risk by implementing controls. This is deemed the most cost-effective approach for the majority of business owners involved in m-commerce today. Companies such as Sybase, Inc., provide end-to-end solution to m-commerce and holistic risk management services. An example of their Sybase m-commerce 365 product together with an example of best practice in mobile financial services are provided to substantiate and exemplify some of the risk reduction approaches.

Mobile banking, mobile payments, and mobile commerce represent a growing and promising class of mobile services for consumers. CTIA, an international association for the wireless telecommunications industry, in association with the leading US wireless carriers, has developed Best Practices and Guidelines (CTIA – The Wireless Association, 2009) to promote clear and rewarding consumer experiences, to establish an environment
where mobile transactions are authorised, secure, and compliant with applicable laws and industry guidelines, and to protect user privacy and financial data.

There are a number of other risk mitigation strategies that a firm can use to effectively reduce legal exposures. Businesses can enhance their disclosure and compliance practices by disclosing, in a clear and conspicuous manner, the material terms of each purchase, including a description of the product or service being purchased, taxes, surcharges, and other fees and refund policies. They can also provide products, services, software, and/or hardware in accordance with all applicable local, state, and federal laws, payment network rules, and mobile industry best practices guidelines. They should disclose to users their access, collection, use, and storage of personally identifiable information. Entities that use information collected to create aggregate data should remove or permanently obscure the consumer’s identity and provide clear notice of such aggregation and use. In the event of a security breach, enterprises should notify consumers of the breach in accordance with relevant breach notification laws.

To successfully secure network and data transmissions and protect businesses from technical risks, technologies such as application access controls, firewall rules, access control lists (ACLs), virtual private network (VPN) guidelines, security monitoring, and antivirus software should be utilised. To this end, mobile device manufactures, wireless application developers, and network providers should draw on decades of progress in securing operating system models and secure models of computation in designing and implementation a safe environment for m-commerce (Ghosh and Swaminatha, 2001).

Business owners should not rely solely on wireless network security. In mobile banking, most security questions centre around how the transaction between payer and payee is protected. Multiple types of communication channels, including mobile must be secured. Banks and mobile operators have the flexibility to assign the level of security and user authentication required based on payment type, transaction value, number of daily transactions and so on. For example, low-risk transactions or communications (e.g., communications with customer service) can be done using a lower level of security, while higher value transactions can be completed over a more secure technology. The higher risk transactions can require a personal identification number (PIN) or out-of-band authentication (e.g., a text message or e-mail to the address on record with the company that contains a second code which must be input along with the user’s password in order to proceed with the transaction). Banks and operator have complete control of the security and risk threshold they want to add for each type of mobile transaction and communication.

To properly safeguard an entity’s assets and sensitive information against physical security risks, businesses should implement intruder detection systems and security firewalls. Additionally, they should protect against unauthorised access to confidential data on a mobile device or in other storage locations. Such protections may include mechanisms for keeping software applications separate, keeping data, and communications secure, and protecting memory from unauthorised access or modification. The combination of dedicated security personal, purpose-built security equipment, and business process protects these facilities from external and internal attacks. In the event of an electrical outage, the site has backup battery power and generators that prevent customer messages from being dropped during a network outage. The site also should have a detailed disaster recovery plan to bring data back online after a man-made or natural disaster. Additional safeguards should be implemented to help limit security breaches in the case of lost or stolen devices. For example, McAfee Wave
Secure is an available product that will locate, remotely lock down and, if necessary, remotely wipe clean a lost or stolen mobile device and will back up the data remotely to the web. It also can locate your mobile device on a map and track SIM cards and calls made to recover the missing mobile device (Siciliano, 2011a). This can decrease both company and consumer risk.

Most importantly, merchants should educate consumers not to store any sensitive data on the mobile device. Transaction limits, cumulative limits and account balance limits protect both customers and mobile commerce providers.

4 Conclusions

As changeable as the world of m-commerce itself, risks involved in this emerging transaction platform evolve every single day. M-commerce service providers need to keep abreast of the latest trend in the dynamic business environment, update their risk awareness and knowledge base, educate their employees and customers, and finally take proactive and corrective actions to mitigate their risk exposures in line with the company’s risk profile.

The imminent risks facing both businesses and consumers come mainly from three sources: technologies, laws, and physical securities. Although hard to avoid, existing risk responsive practices in the more matured e-commerce market can be referenced and tailored to address the specific risks inherent in the m-commerce business, but with the recognition that mobile wireless access poses new and additional risk on the firm. With little doubt, m-commerce is enjoying much wider popularity in the business world. It is worthwhile to mention, however, the great many opportunities related to this business model have not been fully tapped and explored. Insurance companies and other related business partners could spark their creativity and benefit from utilising the risk sharing approach. As long as the risks discussed in this paper are sufficiently cogently evaluated and appropriately addressed, all parties can participate in taking m-commerce to the next step forward while protecting company and consumer risks.

Security is essential if mobile technology is to reach its potential for commerce. Without trust and confidence by consumers, m-commerce is not going to thrive. Breaches, even in secure places like the US Defense Department, or hacking into the digital certificate authority companies (those that issue certificates ensuring that the website accessed is the correct one and not a phishing or pharming scam site) and then producing bogus certificates (Acohido 2011) undermine consumer trust and can derail the growing m-commerce trend. Accordingly, future research should investigate alternative security techniques such as biometric security for mobile devices (face scans, fingerprints, etc.). Multiple layers of security can also help stem the erosion of consumer confidence.

Another line of research is into the economically efficient allocation of risk in mobile commerce. As mentioned previously, the legal system is currently regulating wireless mobile commerce on the basis of previous technologies such as print or television media, and telephone regulations. Risk in m-commerce is not now necessarily born by the entity most responsible for creating (and hence most in control of mitigating) the risk, such as the smartphone producer or application developer. Vulnerabilities resulting in risk created by these producers should leave them liable so as to create incentives for risk mitigation. Precise legal risk transfer agreements in this context are worth investigating in
future research. If producer had this liability they might be more inclined to incorporate biometric security or run security software continuously, even if it slowed down the communication or used battery power more rapidly. Further, power source advancements will eventually make this constraint less important than it is now.

References


Managing risk in mobile commerce


