Near field communications: A change in “frequency”

Mobile devices are increasingly being used to transfer sensitive data, creating exposures for businesses receiving, storing or sending information.

By Larry Collins
Head of E-Solutions
Zurich Services Corporation

More consumers are electing for “wallet-less transactions,” whereby they can use their smart phones, PDAs or other mobile devices to make purchases at sales counters, receive discounts and earn rewards points — rather than digging around for their credit cards, coupons or one of the many customer loyalty cards on their key chains.

Gross transaction volume from mobile payments is expected to reach $630 billion globally by 2014, according to information from the National Retail Federation.

Retailers aside, other businesses are also turning to mobile technology to seamlessly transfer company files or share documents among employees from anywhere in the world.

Businesses that want to stay competitive in their marketplaces will likely need to adopt technology that can support such data transactions — potentially putting unprepared businesses at risk for costly data breaches.

Convenient capabilities, risky ramifications

The heightened risk for data breaches stems from a variety of technological advances including near field communications, which is the wireless technology that enables devices like smart phones — within a short range of other smart phones, point-of-sale terminals or “smart posters” — to exchange data.

Advances in near field communications are driving the trend toward using mobile technology to authorize payments, transfer corporate documents or files, or pass along personally identifiable information to another individual or entity.

Users of near field communication-enabled devices can, in an instant:

- Make payments or use coupons via devices, instead of credit or debit cards.
- Transfer files and share documents.
- Download information about objects, services or places from “smart posters.”
- Display electronic identity documents, like air travel boarding passes.

Such broad capabilities certainly offer conveniences but also elicit questions about the technology’s security, considering the potentially sensitive data being transmitted or the likelihood of a hacker intercepting that information during a live data exchange.

Individuals are not the only parties at risk from having their personal information confiscated. Businesses engaging in mobile data transactions are also at risk, with the potential to be held accountable for any data breaches resulting in the exposure of their customers’ or employees’ personally identifiable information — not to mention any corporate data from shared files or documents that could be lost.

Being smart about smart technology

Companies cannot ignore the potential dangers of a data breach — from financial losses to reputational damage to legal liability. Cyber security was named one of the top five global risks for companies in 2011 at the World Economic Forum in Davos, Switzerland. Further, mobile device use was cited as one reason corporate data has become vulnerable to cyber attacks.

According to the Ponemon Institute's 2011 Cost of Data Breach Study: United States, the average cost of a data breach in 2011 was $5.5 million. Costs often stem from determining the severity and scope of a breach; establishing a call center to manage inquiries from affected parties; legal defense; public relations; regulatory proceedings, fines and penalties; credit or identity monitoring; and notifying third parties of the breach.

Considering the high stakes, companies using near field communications should prepare themselves for the direct costs, as well as the indirect costs, of a data breach scenario by implementing risk management practices.

Businesses that rely on near field communications to share company information can implement these risk management tactics:

- Automatically shut off an employee's smart phone if it's lost, so information can't be accessed by unauthorized parties.
- Enlist the company's telecommunications and information technology department to limit the content that employees can download or store.
- Enforce a password requirement.
- Encrypt data so it can't be easily read.

Businesses that rely on near field communications to accept payment from customers or to acquire information about customers can implement these risk management tactics:

- Use transmitted data for the purpose it was collected. If a customer shared personal information solely to pay for something, don't then use that data for targeted marketing.
- Secure collected data with encryption, passwords and by restricting access.
- Determine how long data should be stored; create a data purging cycle.
- An educated team, aware of global privacy laws, should be in place.
- Limit data-reading devices' power, allowing them to receive data only from short distances.
- Limit the content that devices display during transactions.
- Implement the electronic security measures that a near field system requires.

Assurance with insurance

Risk management tactics are critical to protecting organizations from near-field related data breaches. Still, they are not enough, which is why the use of insurance as a risk management tool is so important.

Many companies mistakenly believe they are covered against data breach events through one of their existing Property and Casualty policies, which are typically triggered by a "claim." Data breaches, however, often don't turn into actual claims that can be filed against a traditional liability policy because of effective breach response or difficulty proving actual damages.

Property policies may not respond to loss of data since "data" is considered intangible, and property policies typically only cover the loss of tangible property. Even if a claim was filed, and a professional liability or commercial general liability policy partially responded, a company would still be held accountable for first party privacy breach costs like forensics, notification, call centers and public relations.

Because of the gaps in these traditional insurance products, more organizations are using cyber risk insurance to mitigate risks associated with near field communications and mobile technology. Cyber risk insurance consists of two types of coverage.

Liability coverage is for claims against an organization brought by third parties that covers defense costs in the event of regulatory proceedings. Coverage is also available for privacy breach costs, business interruption, digital asset loss and cyber extortion.

Protection also can be found in the form of specialized liability insurance, such as Errors & Omissions and Security & Privacy coverage. These coverages go beyond liability insurance to cover management liability and employment practices.

The bottom line

Using mobile devices to pay for a latte, share a work document with a colleague, store corporate credit card data or check-in on a flight offer great advantages to consumers and businesses alike.

At the same time, such capabilities pose risks that could jeopardize an individual's privacy or threaten the bottom line and reputation of a company engaging customers or employees in near field communications — regardless of industry or size.

Companies that traditionally have had little data about their customers now must become accustomed with data privacy and security laws, and protect their customers' personal information. They must also protect company data so as to not reveal trade secrets or financial information.

At the end of the day, though, the newness of near field communications makes it a mystery to many users — making it challenging to anticipate and mitigate all the risks, and furthering the need to explore all risk management tools — including insurance.

Zurich Services Corporation
Risk Engineering
1400 American Lane, Schaumburg, Illinois 60196-1056
800 982 5964 www.zurichna.com

The information in this publication was compiled by Zurich Services Corporation from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich Services Corporation reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.