وأفضل الممارساتوفي كل الحالات ومع أي قناة تسليم جديدة على الإنترنت، يعتبر الأمن هو الواجهة الأمامية للشركات حيث تهرع الشركات إلى استخدام وتعزيز التطبيقات التجارية النقالة في سوق الهواتفالذكية المتنامي، وتختلف أولوياتهم عن أولويات مطوري البرامج المتداولة والناقلة للتطبيقات. في القطاع المصرفي تقتصر معظم تطبيقات الهواتف بالنسبة للعملاء على مجموعة من المهام، منها : مراجعة أرصدة الحساب وتواريخ المعاملات والوصول إلى الفرع أو مكان ماكينة الصراف الآلي أو عمل التحويلات، ولكن الموجة الجديدة من التطبيقات جلبت بعض خدمات الدفع من شخص إلى شخص والإيداع عن بعد ودفع الفواتير من خلال الهاتف وببساطة، أصبحت التطبيقات أكثر ذكاءً وقدرة ولكن على الجانب الأخر جلبت تلك الإمكانيات مزيدا من التهديدات.يذكر خبراء الأمن أن معظم التحديات التي قد تنجم عن الاحتيال عن طريق الجوال لم يتم مشاهدتها من قبل، فالتجارة الإلكترونية عبر الجوال تعتبر أمرًا جديدًا نسبيا وغير مستهدف حتى الآن؛ بيد أن الجاسوسية الصناعية وسرقة الأسرار التجارية من خلال استهداف الأجهزة النقالة آخذة في التصاعد والتركيز على الذكاء التنافسي الاحتيالي يجمع المؤسسات وينبغي أن يكون المستخدمون من المؤسسات أكثر فاعلية ومنهجية وإتقانًا عند تصميم واستخدام تطبيقات الأجهزة النقالة أكثر منهم عند القيام بذلك مع التطبيقات القائمة على الويب.يبحث مطورو البرامج ـ بشكل أساسي ـ ـ عن أوسع نطاق من الجمهور، يتعين على الشركات بناء التطبيقات من أجل نقاط القوة والضعف الأساسية الداخلية لكل جهاز مما يضيف مزيدا من التحديات فيما يتعلق بعملية التأمين.ومن وجهة نظر المستخدم، هناك إحدى الأعراض الجانبية لجهود تطوير تطبيقات الأجهزة النقالة وهو أنها تعيد تشكيل الطريقة التي يتفاعل بها المستخدمون مع تطبيقات إدارة المعلومات الأساسية داخل الشركة. وتعتبر أنظمة إدارة معلومات المكتب الخلفي مثل المحاسبة وإدارة العلاقات مع العملاء والموارد البشرية وتطبيقات الشركة الأخرى التي يجري تشغيلها على الإنترنت وعلى الجوال هي نفسها كما كانت من قبل، ولكن الاختلاف الأكبر يكمن في كيفية تعامل المساهمين (الموظفون والعملاء والموردون) مع الشركة فعندما كان يجري نشر تطبيقات الإنترنت الأساسية لمتصفح الوصول، فقد كان هناك المزيد من التحكم في بيئة التشغيل أما مع التطبيقات النقالة الأحدث التي تعمل على الهواتف الذكية والتابلت تم نقل تلك المهمة إلى أجهزة المستخدمين النهائيين.حوكمة المعلومات للأجهزة النقالةضعف فهم التهديدات الفعلية٣٥٩تتزايد قائمة التهديدات المتعلقة بتطبيقات الأجهزة النقالة، ولكن هناك عدم فهم لتلك التهديدات عامة فهي تعتبر جديدة جدا لأن تجارة الأجهزة النقالة بواسطة التطبيقات القابلة للتنزيل تعتبر ظاهرة جديدة نسبيا وقد تصارعت تطبيقات آبل آي تون ستور و سوق آندرويد" في النصف الثاني من عام ٢٠٠٨ . "لكن ذلك لا يعني أن التهديد غير حقيقي حتى إذا لم يكن التطبيق نفسه هو المشكلة". فالمشكلة قد تكون تشغيل المستخدمين لشبكة غير مؤمنة أو نوع ما من الإصابات من الجهاز. بالنسبة لتطبيقات الأجهزة النقالة، التركيز لا ينصب على الحماية ضد الفيروسات كما هو الحال في عالم الحاسوب الشخصي، وبالتأكيد سوف يستمر وجود أنواع جديدة من الهجمات على الأجهزة وذلك هو الأمر الوحيد الذي ينبغي التحرز له.كشف عن بعض نماذج الأجهزة النقالة ذات المواصفات العالية على سبيل المثال في عام ٢٠١٠: وأن تطبيق آي فون سيتي بنك القائم على نيويورك يقوم بتخزين بيانات العملاء على هواتفهم مع وجود تأثيرات واضحة على الخصوصية [وتعريضها للسرقة والاحتيال] وفي الوقت نفسه تعين على (جوجل، نيويورك) بجلب عدد من التطبيقات من سوق تعاملات آندرويد تم إنشاؤها بواسطة مطور مشابه [مجرم]، الذي أنشأ تطبيقات مصرفية مزيفة [بمميزات واقعية وغير قابلة للاستخدام] تحاول استغلال المعلومات الموجودة على أجهزة المستخدمين لارتكاب جرائم احتيال مصرفية وتزوير بطاقات الائتمان. ويوجد العديد والمزيد من الأمثلة، لكن الحوادث المذكورة تجعل من الضروري والإلزامي تفهم سوق تطبيقات الأجهزة النقالة نفسها من أجل تطوير ونشر وتعزيز سياسات وضوابط حوكمة المعلومات بشكل فعال، فبشكل بسيط معرفة كيف تقبل جوجل على ترويج تطوير التطبيقات هو مفتاح تطوير إستراتيجية حوكمة المعلومات (IG) لأجهزة آندرويد، فطريقة جوجل المفتوحة نسبيا تعني مبدئيا أن أي شخص يمكنه تطوير ونشر تطبيق لصالح آندرويد على الرغم من تطور السياسات نوعا ما لحمايةمستخدمي أندرويد مازال من السهل ـ إلى حد ما ـ على أي مطور تطبيقات حسن النية أو عدمها. وقد يسبب ذلك نفسه مخاطر للمستخدمين النهائيين الذين لا يمكنهم التفريق بين التطبيق الفعلي الصادر من جانب البنك، والتطبيق المصرفي المثبت من جانب طرف ثالث والتي قد تكون احتيالية. ولقد اتخذت آبل نهجًا أكثر احترازا وانضباطا من خلال دعم وتقوية عملية معتمدة ومتحكم في جودتها لكل التطبيقات التي يتم إصدارها إلى متجر تطبيقات آي تونز، وبالتأكيد يبطئ ذلك من عملية التطوير ولكن ذلك يعني أيضا أن كل تلك التطبيقات سوف يجرى اختبارها وتأمينها بدقة وإحكام.٣٦٠حوكمة المعلومات ـ مبادئ، واستراتيجيات، وأفضل الممارساتوجد إيجابيات وسلبيات في كلتا الطريقتين بالنسبة للشركات

ومستخدمي الأجهزة، ولكن من الواضح أن طريقة آبل ـ المتحكم في جودتها والتي يمكن تصحيحها ـ أفضل من نقطة توقع مخاطر التأمين. مفتاح باب الدخول إلى مرحلة تصميم برامج تطبيقات الأجهزة النقالة هو فهم نقاط القوةالكامنة وربما بشكل أهم نقاط ضعف أنظمة تشغيل وأجهزة البرامج النقالة والتفاعل فيما بينها. وتختلف بيئة التطوير تماما وسوف يشهد مبرمجو ويندوز منحنى تعليميا ويجري تشغيلتطبيقات المحمول آندرويد أو آبل في بيئة إدارة ملفات أقل شفافية وأكثر تقييداً. مع مراعاة ذلك ـ بغض النظر عن أنظمة تشغيل OS الجوال ـ ينبغي التأكد أولا من تأمين البيانات ثم مراجعة تأمين التطبيقات نفسها، ومن ممارسات حوكمة تقنية المعلومات IT الجيدة هو التأكد من تأمين كود مصدر البرامج، فقد يتم إدخال كود خبيث داخل البرنامج وبمتصنيف نشر ذلك الكود سيسهل على قراصنة الإنترنت سرقة المعلومات أو البيانات أو الوثائق.الابتكار مقابل الأمن:

الاختبارات والخيارات التفصيلية عندما تنشر أي شركة تطبيق الأجهزة النقالة يتعين عليها عمل خيارات المراعاة بيئة تطوير البرامج المحدودة، أو المقيدة والحاجة إلى توفير تطبيقات أكثر ذكاء وإتقانا حيث تعمل بشكل يقبل عليها المستخدمون. ولضمان أن تكون عروض الأجهزة النقالة مؤمنة تقوم معظم الشركات بـ مهام تطبيقاتها، لذلك يحصل مستخدمو حقوق الملكية على وصول إلى الأجهزة النقالة لم يكونوا يحصلوا عليه من قبل، وواجهة جديدة بمهمة جديدة بيد أنه من غير الممكن تقديم مهام كثيرة،ومزيد من التأمين يعني بعض التضحيات وتوفير بعض الخيارات مقابل السرعة وابتكار سمات جديدة. ومازالت بعض الدروس التي جرى تعلمها عند نشر تطبيقات الويب على الإنترنت، تطبق على تطبيقات المحمول وسيحاول قراصنة الإنترنت استخدام الهندسة الاجتماعية مثل التصيد (الخداع من خلال توفير الوصول أو معلومات خاصة والتظاهر وافتراض هوية حامل حساب أو بنك أو شركة وسيستخدمون أيضا هجوم الوسيط (سنناقش ذلك العنوان بالمزيد من التفصيل لاحقاً). مثل الهواتف الذكية وذلك هو الاختلاف الرئيس بين التطبيقات والواجهات القائمة على الحاسوب الشخصي التقليدي والتي تعتمد على الوصول إلى المتصفح أو استخدام رسائل نصية أساسية على الهاتف الجوال، فالاتصال بالشركة من خلال التطبيق يكون أكثر أمانا من الاعتماد على المتصفح أو منصة النصوص التي تتطلب وصلة إضافية من البرامج (مثل المتصفح أو منصة النصوص أو وصلة واي فاي) لتنفيذ المهام الحساسة، وقد تضر وتكشف جوانب التأمين الضعيفة سلامة المعلومات المنقولة إلى مكان آمنحوكمة المعلومات للأجهزة النقالة٣٦١وإذا تم تطوير التطبيق في بيئة آمنة فيمكن أن يكون التطبيق مكتفيًا بذاته وتتزايد فرصة حفظ البيانات بشكل آمن عند استخدام التطبيق بخلاف المنصات القائمة على المتصفح. وذلك لأن تطبيقات الأجهزة النقالة توفر اتصالا مباشرًا بين جهاز المستخدم والشركة أو الجهة الحكومية أو مزود التجارة الإلكترونية.