西安科技大学

毕业设计(论文)文献翻译

题　　目	Managing mobile security: How are we doing?
院、 系(部)	计算机学院
专业及班级	软件工程0902
姓　　名	王　鑫　骅
指 导 教 师	付　燕
日　　期	2013年03月30日

移动安全管理：我们应怎样去做？

Alan Goode，常务董事，古德情报公司

最新一代的智能手机，例如 iPhone 和 Google 的 Android 系统手机，正对我们访问，使用以及存储信息的方式产生革命性的影响。具有移动数据功能、多网络（移动数据及 WI-FI 功能）、长时间待机的移动设备能带给我们的商业效益已毋庸置疑，但是信息安全的意义是指什么呢？在移动设备上访问公司的机密信息是否为我们敲响了警钟？允许员工在商务中使用他们自己的手机是否为蠕虫病毒开辟了温床？谁拥有这些数据？

《古德情报公司（GI）2009 年移动安全调查》是一个独立于运营商的关于商业活动中手机安全性的研究，它给出了一个关于企业如何解决手机安全性带来的挑战的概览。全文将会以三部分出版，前两个部分已经发行，并且可以在古德情报公司的网站上下载，www.goodeintelligence.com。

有谁参加本次调查？

本次调查的受访者来自各行各业，包括金融，国防，政府，医疗保健，技术，电信，慈善机构，人才招聘，法律，零售和公共事业等。

“只有不到一半的受访者（46%）没有制定明确文档化的覆盖了手机领域的安全政策”

调查受访者来自世界各地：欧盟，欧洲的其他国家以及北美三个地区。受访者的职位从高级管理人员到顾问，并且包含如下人员：首席信息安全官（CISO），网络安全经理，信息系统管理和安全的领头者，安全分析师和信息安全顾问。在组织规模上，从少于 100 个员工的公司到超过 100000 名员工的公司都涵盖在内。

在 2009 年，当得知几乎所有的受访者（96%）有一个记录在案的安全政策时，是很令人振奋的。然而，在关于具有明确的记录在案的覆盖了手机领域的政策的组织的时候，呈现出另一番景象。只有不到一半的受访者（46%）没有明确的记录在案的覆盖了手机领域的安全政策。

在回答“如何在移动领域充分地制定像 ISO 27001/2，COBIT 以及 ISF SoGP 那样的安全标准及框架”的问题是，45%的受访者说，移动领域几乎甚至是完全没有被覆盖到。只有 10%的人认为这些标准很好地涵盖了移动安全领域。超过 30%的人表示这些标准充分

地覆盖了移动安全领域，但仍有上升空间。这是个有趣的数据，它指出了正是认识到一个更广泛的问题中包含的信息安全标准和框架，在这些标准中的确存在为手机所预备的部分。

具体而言，ISO 27002 在 11 年 7 月 1 日的移动计算和通信大会中涵盖了移动安全政策，并指出“正式的政策要到位，并应采取适当的保安措施，以防止使用移动计算和通信设施的风险”。此外，ISF 将移动设备（PDA 等）加入了 SoGP 标准，特别是 SM5.2.2，CB3.3.4，C12.8.6 和 UE6.3.1。

手机安全意识

显然，拥有成文的政策是必不可少的，但政策的成功执行，更加需要确保用户意识到这一点，以及当他们参与到每天的商务活动中时坚持下去。关于这一点，调查的结果是令人鼓舞的。然而，大多数受访者认为，使用户意识到安全政策的必要性并确保其得到实施，还有很多工作要做。

“随着基于手机的应用的爆炸式增长，与之相关的安全危机也不可避免，就如所报道的一样，Android 系统的木马，09Droid，产生了。”

在 54%的拥有详细成文的涵盖手机领域的安全政策的机构中，，50%的人认为他们的用户了解协议，17%的人认为不了解，剩下的 33%中表示他们并不确信用户是否了解。

移动安全策略

为了有效，移动安全已被纳入一个组织的整体安全战略。从信息安全的专业人士那里，征询道德这种情况的发生，也有一些令人鼓舞的迹象。

超过一半的受访者（53%）表示，手机安全是他们的整体安全策略的“非常重要”或是“重要”的一部分。其余的 47%则表示“不很重要”。没有人说它是“完全不重要的”。

安全性和移动手机应用程序部署

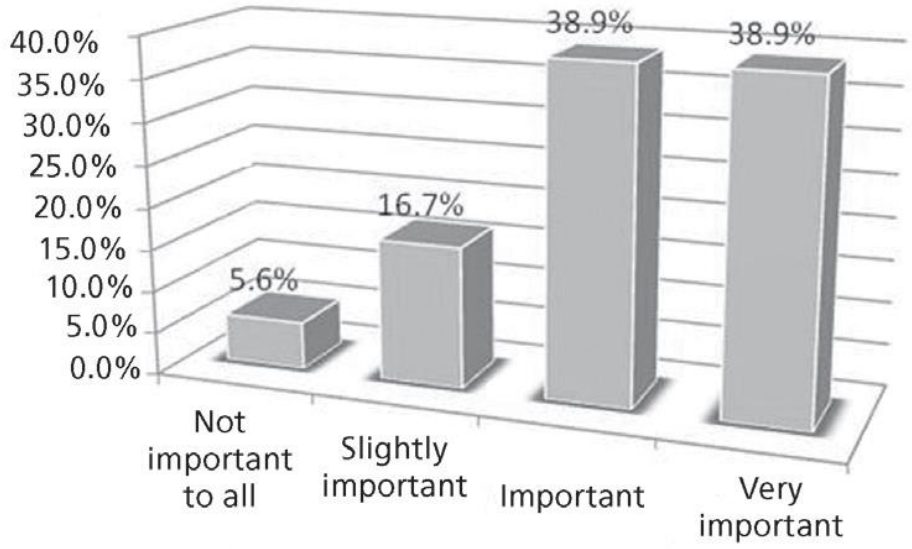

图 1：移动安全在手机应用部署中的重要性

苹果公司的 iPhone 和谷歌的 Android 手机正在改变我们使用手机的方式，这更强调了移动应用程序的重要性。苹果通过 iTunes 分布的移动应用程序商店，和谷歌的 Android 市场，都在改变手机行业的面貌。

随着基于手机的应用的爆炸式增长，与之相关的安全危机也不可避免，就如所报道的一样，Android 系统的木马，09Droid，产生了。调查的目标之一是要找出在部署手机应用的过程中，移动安全有多么重要。

大多数人——几乎 78%——感觉到移动安全在手机应用部署过程中“非常重要”或“重要”，只有 5%的人认为移动安全在部署应用中“并不重要”。

用于商业目的的员工的手机

65%的受访者表示，他们允许员工拥有的移动电话用于商业用途（包括语音通话，手机邮箱，移动企业应用程序）。这是一个很高的数字，后果则是管理由手机带来的信息安全问题。信息安全部门如何能执行移动安全策略和技术性地控制私人所有物？此外，如果一个信息安全部门正在部署一个基于手机的身份验证解决方案，例如把手机当作双重认证（2FA）令牌，那么在非企业的设备上安装安全软件的后果是什么？

手机和网络访问——本地网络

智能手机在企业中使用率的上升正推动着允许这些设备连接到本地网络的需求上升。流动性在工作空间在工作中是同等重要的，就像是在远程办公一样。在线办公及定期会议的意思是，我们需要在任何工作场合访问企业的信息，有时是不可行的，或是带一台笔记本电脑到办公室里。

iPhone 和无处不在的黑莓手机已经成为会议桌上必不可少的工具。调查显示，30％的企业目前支持手机上的本地数据网络。另有 12%的企业目前不支持此功能，但计划在未来 12 个月内部署。 58％的企业由于各种原因不支持在本地网络使用移动电话。

手机和网络访问——远程访问网络

最新的移动电话和智能手机设备让企业用户能够访问一些最重要的业务应用程序，如电子邮件，销售队伍自动化工具，财务分析工具等。在移动中访问最先进的最新信息已经成为当今的移动员工必须具备的技能。被认为是工作和社会生活的边界越来越模糊，例如，在商务旅行和私人假期中访问企业数据很多时候都很有必要。

因此，约有 42％的组织允许让手机远程连接到企业数据网络。其余 58％的企业不允许员工使用他们的手机来访问企业网络。

这种情况的原因如下：56％的受访者表示，他们没有商业上的理由允许连接；33％的人表示，信息安全政策，以及可能的调控，阻止他们允许访问；剩下的 11％表示，他们没有技术支持手机远程访问他们的网络。

手机作为身份验证设备

在 GI 的报告《手机作为身份验证设备》,《2010-2014 分析与展望》中，列出了手机作为 2FA 硬件替代品的许多好处，例如：

大幅节省成本

有效地分布和管理

易于使用的优点

部署优势

该调查询问了通过手机作为组织内的认证设备的问题。目前没有受访者使用手机作为身份验证设备，但最重要的是，40％的受访者计划部署它。所有这些都计划到 2011 年

底将其部署。

还有 66%的那些目前没有使用手机作为身份验证设备的组织，认为目前还没有理由来接受这样的连接，9％的人表示，政策阻止他们使用这种技术，其余 25％的受访者表示有“其他'的原因。这些“其他”的原因给出了一个这种技术不能被大规模应用的有趣的观点，包括：

并非所有的企业都有企业手机

在世界一些地区的网络覆盖差

关注 SMS 足够可靠和安全的运输 OTP

手机和病毒

从在 2009 年年底出现了好转的新闻故事手机的潜在威胁，特别是智能手机，从感染病毒和恶意软件的数量。

GI 移动 2009 年安全调查询问组织有过感染收集病毒的经历，以及如果他们意识到威胁，会采取任何措施来对付这种威胁。

“目前没有受访者使用手机作为身份验证设备，但最重要的是，40％的受访者计划部署它。所有这些都计划到 2011 年底将其部署。”

本次调查结果为 GI 关于手机防病毒产品及服务的分析报告提供了有价值的定量数据。这份报告分析了基于手机的防病毒（AV）产品和服务，包括部署在移动运营商，移动应用和内容提供商的市场中的端点解决方案和基础设施产品和服务。

至于手机反病毒产品和服务方面，调查发现，目前只有 13％的组织在保护他们的移动电话免于手机病毒的威胁。而超过一半（54％）的人当被问及是否正在针对手机病毒的威胁保护自己的手机时回答道“目前没有，但正在计划”。在这 54％中，有三分之一（33%）接受调查的机构表示，他们将在未来 6 个月的部署移动 AV（2009 年 9 月-2010 年 3 月）。剩下的三分之二（67％）的受访者表示他们将在“6 个月至 12 个月内”部署移动 AV（2010 年 4 月）。

手机数据加密

在回答“你正使用数据加密产品来保护存储在设备中的数据吗”时，27%的组织回答

“没有”。 33％的企业正在使用加密产品来保护员工的手机，余下的 40％正在计划部署的手机加密产品。所有这些 40％的计划部署的机构都计划从 2010 年 9 月起部署。

手机备份

目前，27％的受访者正在使用针对存储在手机中的数据的备份技术。绝大多数（73％）并不备份存储在手机上的数据，并且没有组织计划在未来两年内实施这项技术。

手机的违规行为和事件 – 来自手机的未经授权的网络访问

手机有能力进入一个组织的网络发动攻击。他们有 Wi-Fi 功能，足够的存储空间，可执行应用程序，很容易隐藏。许多组织都进入一个保密的环境前要求上交手机（主要是因为相机的功能）。

当回答“为什么你们不会部署手机备份技术”的问题时，64%的企业回答说“员工手机上的数据无需备份”

在回答“你曾经尝试过使用手机进行未经授权的网络访问吗？”时，绝大多数的受访者（87％）指出：“没有。”剩下的 13％说他们“不知道”。组织是否有能力监视和控制手机访问他们的网络是一个不得不考虑的问题。此外，手机能够通过 USB 或蓝牙与电脑进行同步也是一个值得考虑的问题。

手机违规行为和事件 - 手机病毒的证据

手机病毒已经存在很多年了，但一直没有造成手机用户实际的恐惧。但这也许会随着许多安全评论员把 2010 年视为“移动病毒之年”而改变。

如今已有许多被广泛宣传的手机病毒感染事件，尤其是 2009 年 11 月报道的关于苹果公司 iPhone 越狱的两起攻击。这两个蠕虫病毒是 Ikee，首次被发现是在澳大利亚，并且攻击了荷兰银行 ING 的客户。

GI 想要知道是否有组织在 2009 年时对移动电话的安全进行过民意调查时又无证据表明手机病毒感染了他们员工的手机。由于仅有 13%的组织真正保护他们员工的手机免受手机病毒的威胁，因此“是否组织或员工能确切知道手机是否被感染”这一问题就亟需

回答。

绝大多数受访者（几乎 87%）没有手机感染病毒的证据。差不多 7%的受访者回答“是”并且曾有过员工手机被病毒感染的经历。剩下的 7%回答“不确定”是否感染过手机病毒。这很好地证明了他们没有科学手段监控手机病毒。

总结和展望

手机安全信息安全领域一门新兴的学科，并且 GI 2009 年的手机安全调查使我们了解了各种组织当前的移动安全状态。调查结果肯定了目前在信息安全领域的预测，即在企业内部使用手机会带来安全方面的挑战和威胁，并且这些威胁将在未来几年内变大。

GI 建议，社会需要采取以下步骤，以确保能够应对这些挑战：

教会他们自己处理威胁

在政策和处理流程中反射出这种威胁

确保安全性插入采购程序购买的手机

澄清这一问题上使用的个人移动电话公司的业务

部署适当的技术控制

监测策略和技术控制的有效性

关于作者

艾伦·古德是古德情报的创始人和董事总经理。他是一个受人尊敬的信息安全和移动商务专家，并写了一份有关这些主题的报告。在此之前，艾伦在移动电子商务和信息安全产业的龙头企业担任高级管理职务超过 20 年，包括 T-Mobile 英国公司，摩托罗拉公司，De La Rue 酒店，花旗银行，斯伦贝谢公司和 Atos Origin 公司。

Managing mobile security: How are we doing?

Alan Goode, Managing Director, Goode Intelligence

The latest generation of mobile phones, such as the iPhone and Google's Android platforms, are having a transformational effect on the way that we access, use and store information. There is no doubt of the business benefit that data-enabled, multi-network (mobile operator and Wi-Fi enabled), always-on mobile devices give us but what are the implications for information security? Does access to company-confidential information on a mobile phone give us cause for alarm and by allowing employees to use their own phones for business are we opening up a compliance can of worms? Who owns the data?

The Goode Intelligence (GI) mobile security 2009 Survey is a vendor-independent study of the current status of mobile phone security within business, providing a snapshot of how business is tackling the security challenges posed by mobile phones. Published in three parts, the first two parts have been published and are available to download from the Goode Intelligence website, www.goodeintelligence.com.

Who took part?

The survey respondents came from a wide cross-section of sectors including finance, defense, government, healthcare, technology, telecommunications, charity, recruitment, legal, retail and utility.

"Just under half of the respondents (46%) do not have a specific documented security policy that covers mobile phones"

Survey respondents came from three regions around the world, the European Union, the rest of Europe, and North America. The role of the survey respondents ranged from senior management to consultant and included the following: chief information security officer (CISO), network security manager, head of IS governance and security, security analyst and information security consultant. In terms of organizational size, there was representation from companies with fewer than 100 employees through to those with more than 100 000

employees.

It is heartening to learn that in 2009, virtually all of the respondents have a documented security policy (96%). It is another story however, regarding organizations that have a specific documented security policy that covers mobile phones. Just under half of the respondents (46%) do not have a specific documented security policy that covers mobile phones.

In answer to the question 'how adequately do security standards and frameworks such as ISO 27001/2, COBIT and ISF Standard of Good Practice (SoGP) cover mobile?' 45% said that mobile was covered slightly or not at all. Only 10% stated that the standards cover mobile security policy well. A further 30% reported that the standards covered mobile security policy adequately but that there was room for further improvement. This is an interesting statistic, and points to a wider issue of awareness of exactly what is contained in information security standards and frameworks, as provisions for mobile phones do exist in these standards.

Specifically, ISO 27002 covers mobile security policy in 11.7.1 Mobile computing and communications and states that a "formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities". Additionally, ISF covers Mobile devices (PDAs) in the Standards of Good Practice (SoGP), specifically SM5.2.2, CB3.3.4, C12.8.6 and UE6.3.1.

Mobile security Awareness

Clearly it is essential to have a documented policy but crucial to the success of implementing the policy is ensuring that users are aware of it and critically, adhere to it when they go about their day-to-day business. The results from the survey are encouraging with regard to this. However most respondents felt that more work needs to be carried out in making users aware of security policy and ensuring that the policies are followed.

"Inevitably with the explosion in mobile phone based applications there are associated security risks, as the reported Android Trojan, 09Droid, demonstrates"

Of the 54% that do have a specific documented security policy that covers mobile phones, 50% stated that they thought their users were aware of policy, 17% felt that their users were not

aware, while the remaining 33% stated that they were not sure whether their users were aware.

Mobile security strategy

To be effective, mobile security has to be incorporated into the overall security strategy of an organization. There are some promising signs from the information security professionals that were canvassed for this survey that this is happening.

Over half of the respondents, 53%, stated that mobile security was either a ‘very important’ or ‘important’ part of their overall information security strategy. The remaining 47% stated that it was a ‘slightly important’ component of their overall information security strategy while none said that it was ‘not important at all’.

Security and mobile phone application deployment

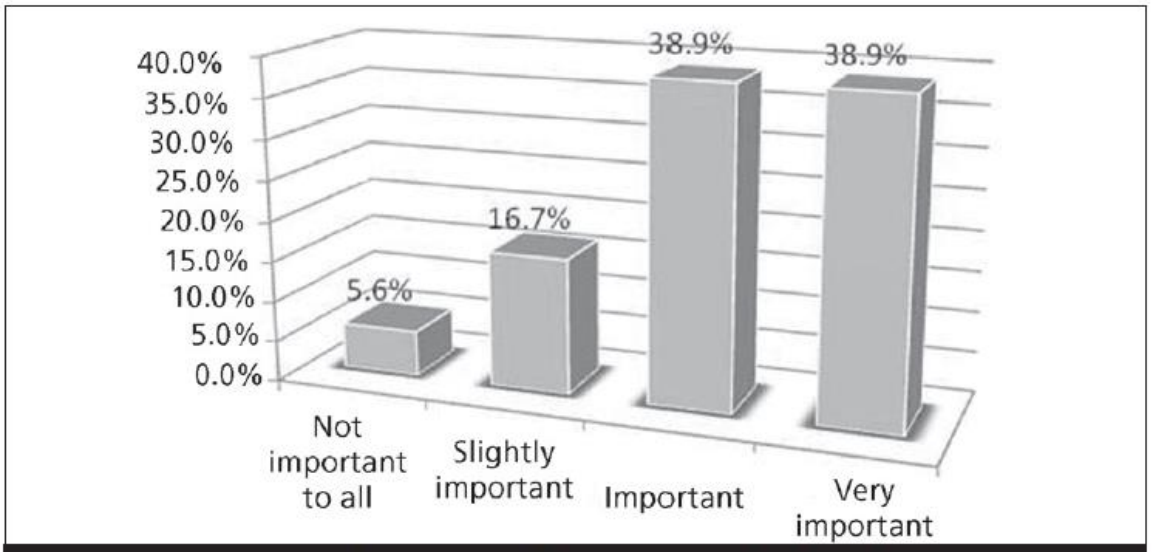

Figure 1: How important is mobile security in deploying mobile phone based applications?

The Apple iPhone and Google Android based mobile phones are changing the way we use mobile phones and this is emphasized in the importance of mobile applications. Apple’s mobile app store, distributed through iTunes, and Google’s Android Marketplace are changing the face of the mobile phone industry.

Inevitably with this explosion in mobile phone based applications there are associated

security risks, as the reported Android Trojan, 09Droid, demonstrates. One of the survey objectives was to find out how important mobile security is in deploying mobile phone based applications.

The majority, almost 78%, felt that mobile security is ‘very important’ or ‘important’ in the deployment of mobile phone based applications with only 5% who considered that mobile security is ‘not’ important at all’ in deploying mobile phone based applications.

Employee-owned mobile phones used for business purposes

65% of respondents stated that they allowed employee-owned mobile phones to be used for business use (where business use includes voice calls, mobile email and mobile enterprise applications). This is a significantly high figure and one that has consequences for managing the information security threat posed by mobile phones. How can an information security department enforce mobile security policy and technical controls that are in private ownership? Additionally, if an information security department is deploying a mobile phone based authentication solution – e.g. the mobile phone as a two-factor authentication (2FA) token – what are the consequences for installing security software on a non-enterprise device?

Mobile phones and network access – local networks

The rise in the use of smartphones within the enterprise is driving the demand to allow these devices to be allowed onto the local network. Mobility is equally as important within the workplace as it is whilst working remotely. Hot-desking and regular meetings mean that we require access to enterprise information in all places of the workplace and sometime it just isn’t feasible or preferable to carry a laptop around the office.

The iPhone and the ubiquitous Blackberry have become the must-have business tools to be placed on the meeting room desk. The survey shows that 30% of organizations currently support mobile phones on their local data networks. A further 12% do not currently support this functionality but are planning to deploy within the next 12 months. 58% of organizations do not support the use of mobile phones on their local networks with varied reasons.

Mobile phones and network access – remote access to networks

The latest mobile phone and smartphone devices allow enterprise users to access some of the most important business applications, such as email, sales force automation tools, financial analysis tools etc. Accessing the most up-to-date information on the move has become a must-have feature for today's mobile employee. The boundary for what is considered to be work and social life is increasingly blurred and it is often necessary to access enterprise data whilst on business trips and private holidays for example.

As such, some 42% of organizations allow mobile phones to remotely connect into the enterprise data network. The remaining 58% of organizations not allow their employees to access the enterprise network using their mobile phones.

The reasons for this are as follows: 56% of respondents stated that they had no business reason to allow connectivity, 33% stated that that information security policy, and possibly regulation, was stopping them for allowing access and 11% said that they didn't have the technology to support mobile phones to remotely access their networks.

The mobile phone as an authentication device

During research for the GI report The Mobile Phone As An Authentication Device; Analysis and Forecasts 2010- 2014, a number of significant advantages were found for using a mobile phone as a 2FA hardware replacement including:

Substantial cost savings
Distribution and management efficiencies
Ease of use advantages
Deployment advantages

The survey asked questions about the adoption of the mobile phone as an authentication device within organizations. None of the respondents currently use a mobile phone as an authentication device but crucially, 40% plan to deploy it. All of these plan to deploy it by the end of 2011.

66% of those who do not currently use the mobile phone as an authentication device cited that there was no current business reason to allow connectivity, 9% stated that policy prevented them from using this technology and the remaining 25% said that there were ‘other’ reasons. These ‘other’ reasons give an interesting insight into key inhibitors for the wide scale adoption of this authentication technology and include:

Not all businesses have corporate mobiles

Poor network coverage in some parts of the world

Concerns over SMS being reliable and secure enough to transport an OTP

Mobile phones and viruses

From late on in 2009 there has been an upturn in the number of press stories about the potential threat to mobile phones, in particular smartphones, from infection by viruses and malware.

The GI mobile security survey 2009 questioned whether organizations had experienced mobile phone viruses and if they were aware of the threat and had taken any measures to counteract that threat.

“None of the respondents currently use a mobile phone as an authentication device but crucially, 40% plan to deploy it. All of these plan to deploy it by the end of 2011”

The survey results contribute valuable quantitative data to the GI Analyst Report Mobile Phone Anti-Virus Products and Services – Analysis and Forecasts 2010- 2014. This report analyses the market for mobile phone-based antivirus (AV) products and services, including endpoint solutions and infrastructure products and services, deployed by mobile operators, mobile application and content providers.

In terms of adoption of mobile phone anti-virus products and services, the survey discovered that currently only 13% of organizations are protecting their mobile phones from the threat of mobile viruses. Well over half, 54%, answered ‘not at the moment but planning to’ when asked whether they currently protected their mobile phones against the threat of mobile phone viruses. Of these 54%, One-third of organizations polled, 33%, said that they would be deploying

mobile AV in the ‘next 6 months’ (September 2009-March 2010). The remaining two-thirds of respondents,

67%, stated that they would be deploying mobile AV within ‘6 to 12 months’ (April-September 2010).

Mobile phone data encryption

In answer to the question ‘Do you currently use data encryption products to protect information stored on the device’ 27% of organizations stated ‘no’. 33% of organizations are currently protecting their employees mobile phones with encryption products and the remaining 40% are planning to deploy mobile phone encryption products. Out of these 40% of organizations that are planning to deploy mobile phone encryption products, all of them, 100%, plan to deploy from September 2010 onwards.

Mobile phone backup

Currently 27% of the respondents are currently using backup technology that targets data stored on a mobile phone. The vast majority, 73%, do not backup data stored on mobile phones and no organization plans to implement this technology within the next two years.

Mobile phone breaches and incidents – unauthorized network access originating from a mobile phone

Mobile phones have the capability to launch an attack into an organization’s network. They have Wi-Fi capability, adequate storage, can execute applications and are easy to conceal. Many organizations require you to hand in your mobile device before entering a secure environment (mainly because of the camera functionality).

In answer to the question ‘why will you not deploy mobile phone backup technology’, 64% stated that the ‘data on employee phones does not require backup’.

In answer to “Have you experienced unauthorized network access originating from a mobile phone?” the vast majority of respondents (87%), stated ‘no’. The remaining 13% said that they

were ‘not sure’. It must be considered whether organizations have the capability to monitor and control mobile phones attempting to access their network.

Additionally there is also the issue of a mobile phone having the ability to synchronize into a computer using either a USB or a Bluetooth connection.

Mobile phone breaches and incidents – evidence of mobile phone virus

Mobile phone viruses have been around for a number of years but have not yet posed a real and credible threat to mobile phone users. This could well change with many security commentators seeing 2010 as “the year of the mobile virus”.

There have been a number of very well publicized incidents where mobile phones have been infected by viruses. In particular two attacks were reported in November 2009 on jail broken Apple iPhones. The two worms were Ikee, first discovered in Australia, and its variant, Duh, attacking customers of the Dutch bank ING.

GI wanted to discover whether any of the organizations that were polled in the mobile security survey 2009 had any evidence that mobile viruses had infected their employees’ mobile phones. As only 13% of organizations actually protect their employees’ devices against the threat of mobile viruses the question ‘would an organization, or employee, actually know whether a mobile phone has been infected or not’ has to be asked.

The vast majority of respondents, nearly 87%, have no evidence of viruses on mobile phones. Almost 7% answered ‘yes’ and stated that they had experienced a virus on their employees’ mobile phones. The remaining 7% answered that they were ‘not sure’ if they had experienced mobile phone viruses. This may well point to the fact that they have no technology controls to monitor mobile phone viruses.

Summary and outlook

Mobile phone security is an emerging discipline within information security and the GI mobile security 2009 survey enables us to understand the current status of mobile security within a diverse range of organizations. The results of the survey certainly back up the current

feeling within the information security community that the use of mobile phones within the enterprise will bring security challenges and that these threats will rise over the coming years.

GI recommends that the community needs to take the following steps to ensure that these challenges are met:

Educate themselves on the risks

Reflect the risks in policy and procedure

Ensure that security is inserted into procurement procedures for the purchase of mobile phones

Clarify the issue on use of personal mobile phones for company business

Deploy appropriate technology controls

Monitor effectiveness of policy and technology controls

About the author

Alan Goode is the founder and managing director of Goode Intelligence. He is a respected expert in information security and mobile commerce and has written a number of reports on these subjects. Prior to this, Alan spent over 20 years in the mobile commerce and information security industry where he held senior management positions for leading organizations including T-Mobile UK, Motorola, De La Rue, Citibank, Schlumberger and Atos Origin.