References

1. 802.11, Wikipedia, Jan 25 2010 <http://en.wikipedia.org/wiki/IEEE_802.11>
2. UK Frequency Allocation Table, National Frequency Planning Group, 2008 <http://www.ofcom.org.uk/radiocomms/isu/ukfat/ukfat08.pdf>
3. Man arrested over wi-fi 'theft', BBC News, August 22 2007, http://news.bbc.co.uk/1/hi/england/london/6958429.stm
4. Communications Act 2003, Office of Public Sector Information, 2003, <http://http.hmso.gov.uk/acts/acts2003/20030021.htm>
5. IEEE Std 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications, IEEE, 1997, http://ieeexplore.ieee.org/search/freesrchabstract.jsp?arnumber=654749&isnumber=14251&punumber=5258&k2dockey=654749@ieeestds&query=%28802.11+1997%29%3Cin%3Emetadata&pos=0
6. Backtrack 4 download page, BackTrack Linux, Accessed January 2010, <http://www.backtrack-linux.org/downloads/>
7. Change (Spoof) MAC Address on Windows 2000, XP, 2003, VISTA, 2008, KL Consulting, Accessed January 2010, <http://www.klcconsulting.net/change_mac_w2k.htm>
8. Church of Wifi Uber coWPAtty lookup tables, Church of WiFi, April 5 2009, <http://www.churchofwifi.org/default.asp?PageLink=Project_Display.asp?PID=90>
9. WPA Cracker, Accessed January 2010 <http://www.wpacracker.com/>
10. EAP, Wikipedia, January 8 2010, <http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol>
11. 802.1x, Wikipedia, 24 January 2010 <http://en.wikipedia.org/wiki/802.1X>
12. Martin Beck and Eric Tews, Practical Attacks Against WPA, November 8 2008, <http://dl.aircrack-ng.org/breakingwepandwpa.pdf>
13. CCCP, Wikipedia, January 10 2010, <http://en.wikipedia.org/wiki/CCMP>

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 WiFi 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, defence, 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 organisational 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 organisations 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 con-

tained 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.

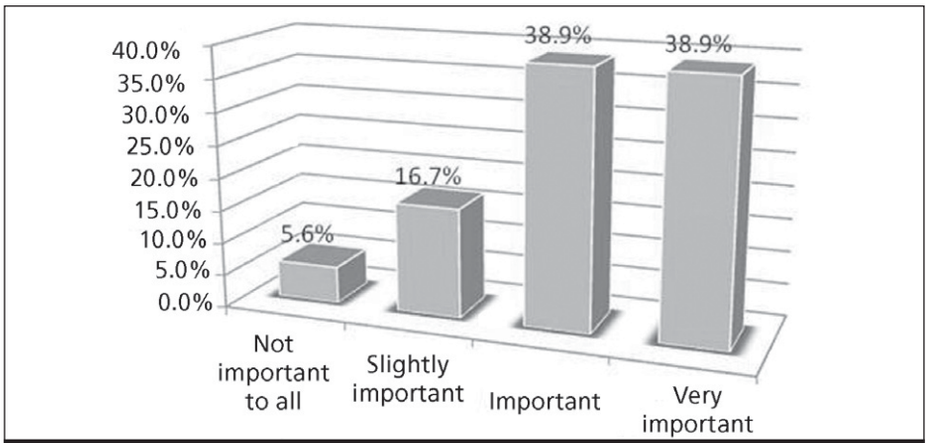

Figure 1: How important is mobile security in deploying mobile phone based applications?

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 organisation. 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

The Apple iPhone and Google Android-based mobile phones are changing the way we use mobile phones and this is emphasised 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 sometimes 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 organisations 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 organisations 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 organisations allow mobile phones to remotely connect into the enterprise data network. The remaining 58% of organisations 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 organisations. 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 organisations 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 organisations 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 organisations 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 organisations stated 'no'. 33% of organisations 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 organisations 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 organisation plans to implement this technology within the next two years.

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

Mobile phones have the capability to launch an attack into an organisation's network. They have WiFi capability, adequate storage, can execute applications and are easy to conceal. Many organisations 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 unauthorised 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 organisations 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 synchronise 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 publicised incidents where mobile phones have been infected by viruses. In particular two attacks were reported in November 2009 on jailbroken 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 organisations 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 organisations actually protect their employees' devices against the threat of mobile viruses the question 'would an organisation, 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 organisations. 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 organisations including T-Mobile UK, Motorola, De La Rue, Citibank, Schlumberger and Atos Origin.

Cybercrime - A game of cat and mouse in 2009

Danny McPherson, chief security officer, Arbor Networks

Last year saw the rapid evolution of complex security challenges. The internet engineering and security communities struggled against a wide range of threats including high DDoS attack rates, IPv6 adoption as well as the growing complexity of cloud and distributed infrastructures. Arbor Network's fifth annual 'Worldwide Infrastructure Security Report' (WWIR), a year long industry-wide operational security survey found some startling statistics and trends.

Attacks shift to the cloud

The survey revealed that nearly 35% of respondents believe that more sophisticated service and application attacks represent the largest operational threat over the next 12 months, displacing large scale botnet-enabled attacks, which came in second this year at 21%.

Again, more than half of the surveyed providers in 2009 reported growth in service-level attacks at one gigabit or less bandwidth levels. Such attacks are also driven by botnets and are specifically designed to exploit service weaknesses, like vulnerable and expensive back-end queries and computational resource limitations.

Several ISPs reported prolonged (multi-hour) outages of prominent internet services during the last year due to application-level attacks. These service-level attack targets included distributed domain name system (DNS) infrastructure, load balanc-