Britain's Culture of Carelessness with Mobile Devices

A survey report exploring London's security 'blackspots' where data is at risk to hackers and thieves

Executive summary

An increasing proportion of the UK population is 'always-on', accessing business and personal information while on the move from mobile devices. Yet many of us aren't aware of the risks of associated with accessing this data outside of the office environment, often leaving ourselves vulnerable to intrusion from cybercriminals who want to get hold of this data for financial gain.

Trend Micro partnered with Vision Critical to investigate how the British public views mobile security and the places that business travellers are most likely to lose data, both through their own actions or through targeting from cybercriminals, such as London train stations, coffee shops or airport lounge.

The research has revealed a worrying attitude of negligence towards work devices from the British public with over a quarter of smartphone users (27%) having had up to three work devices lost or stolen. This is particularly disturbing as over half (52%) of Brits regularly carry a mobile device around with sensitive work data, putting their company and customers at risk of fraud.

The report also reveals that over half (57%) of people who carry a work smartphone have no security protected passwords for sensitive business data, and over a third of respondents don't know what the company procedure is after loss or theft of their device, with just 10% notifying their IT department.

To add weight to the quantitative findings, Trend Micro partnered with the Centre for Creative and Social Technologies (CAST) at Goldsmiths, University of London, to conduct a qualitative experiment with an ethical hacker at First Base Technologies to 'pressure test' these busy commuter spots in Central London and determine how easy it is to hack into mobile devices and what data they can access. Interviews were conducted with the general public to gauge their feedback.

This report explores these findings in more detail and provides advice for businesses to help them protect their staff and devices from being exposed to data theft.

Introduction

Britons are fully equipped when it comes to devices: most of us have at least one of a smartphone, tablet or laptop, and many of us have more than one – our own devices plus those provided by work.

Given the myriad of ways cybercriminals can steal data, you'd have thought we'd be pretty security-conscious about those devices, taking care to password-protect them and not use them in places we can be vulnerable to attack, either from a cybercriminal stealthily snooping on what you're doing or from a thief out to steal your device.

Our devices can carry our entire lives. Contacts, emails, photographs, music – all of those are precious. Many of us also use our devices for online banking.

Work devices can also contain sensitive information – confidential data that shouldn't fall into a rival's hand - and HR details.

Yet it seems that many of us don't bother to take security precautions with our devices, and don't know how to guard against data theft.

And many of us use one device for both work and personal purposes, thanks to the rise of BYOD – bring your own device – in enterprise. Businesses are increasingly allowing their workers to use their own phones, laptops and tablets to access work networks and data, which means that any stolen or unprotected device can be a treasure trove of information to a thief.

But just how much care are we taking of our gadgets? Trend Micro carried out a survey of nearly 2,500 people in the UK to find out how we look after our devices, and found that we are not as careful with our devices and the data they hold as we should be.

Should IT departments be worried?

In short, yes. A total of 20% of the respondents said they use their smartphone for both work and personal purposes, with just 2% saying that their device was a work-only phone, while 24% use their laptop for both personal and work purposes. That means a lot of devices that mix business and personal information which are thus even more of a worry if they go missing.

Yet most of the respondents aren't sure what to do to protect the data on their devices if they're lost or stolen: 29% said they didn't know what to do, and a further 27% said they weren't sure what to do.

When presented with a list of options about what they would do if they discovered their work device had been stolen, worryingly, only 10% said the first thing they would do is notify the IT department. A total of 13% said they would let their boss know, while just 5% would let the HR department know. Most (19%) said they would report the loss to the police first.

Rik Ferguson, global vice-president of security research at Trend Micro, says: "If a work device is stolen, the first people who need to know are the IT department. They can lock and wipe a device – and they need to act quickly."

How secure is your device?

The survey reveals that many of us don't take enough care about password-protecting our data. 63% said they have no password at all on their devices – and, worryingly, 61% of those who use a smartphone for work only said they don't have security passwords on their devices.

Passwords are often a weak link, not least because we're not very good at making sure we use different passwords for each log-in. Of the respondents, 34% said they use the same or similar passwords for both business and personal use, while 28% said they always or mostly use the same password for all their log-ins.

A further 35% said that while they use different passwords, they are nonetheless all quite similar – meaning that if a thief cracks one password, he's more likely to be able to crack them all.

One of the simplest things you can do to thwart a thief if your device is stolen is to use a password lock, but only 43% said that they do on their smartphone. More worryingly, of those using a device solely for work, only 54% said they use a password lock – something that an IT department can force, but not all seem to be doing so. Says Rik Ferguson: "A password lock is the easiest and most effective mechanism. Everybody should be using it."

Not bothered?

Just as concerning is the fact that many of us aren't worried about losing information with a device, both work and personal. Over a quarter of smartphone users (27%) have had up to three work devices lost or stolen and just 16% said they worry a lot about losing professional information such as HR details, with 37% saying they don't worry at all. A total of 47% don't worry much or at all about losing client or customer details, while 55% don't worry much or at all about losing work information about intellectual property.

More of us are concerned about losing personal information: 30% worry a lot about losing their contacts or photographs, while 23% said they feared losing their photographs if their device were lost or stolen. Just 3% said they feared other people having access to important business data, and only 2% worried about what impact losing their device would have on their job.

Unfortunately the repercussions of such an event have become a reality in a number of instances:

- In July 2012 the Ministry of Justice lost, on public transport, data on offenders. The data was handed in to a local newspaper with personal information relating to offenders and third parties. Documents included prison and probation reports, and a total of 66 personal records. The loss was reported to the police and the documents were recovered. Later, in January 2013, an incorrect copy of court hearing lists was emailed from a Cambridge Magistrates Court in error and published on a public website. It had 81 records with names and details of individuals including victims and offenders.

- More recently, in June 2013, Glasgow City Council was fined £150,000 after losing unencrypted laptops, one with personal information of more than 20,000 people including in excess of 6,000 individuals' bank account details. Three years previously, the Council had been given an enforcement notice after an unencrypted memory stick with personal data was lost – proving that a 'shock' does not necessarily concentrate the minds of public sector management. The Council had issued several staff members with unencrypted laptops after problems with encryption software. The ICO discovered that a further 74 unencrypted laptops were missing, at least six of which were known to have been stolen.

- Digital media, which is often not necessarily thought of as containing 'data', can also prove costly. In February 2013, the Nursing and Midwifery Council was fined £150,000 after losing three DVDs related to a nurse's misconduct hearing, which contained confidential personal information and evidence from two vulnerable children. An ICO investigation found the information was not encrypted.

- Even the police themselves can end up in hot water. In October 2012 Greater Manchester Police was fined a hefty £150,000 for failing to take appropriate measures against the loss of personal data. A memory stick containing sensitive personal data was stolen from an officer's home. It had no password protection and contained details of more than a thousand people with links to serious crime investigations. The ICO found that a number of officers across the force regularly used unencrypted memory sticks.

Out and about

We are not careful enough about how we use our devices in public. Despite the inherent lack of security in using public wifi hotspots, 22% of the respondents say they access business emails in public places, while 10% access confidential documents.

And many are happy to use public hotspots, with 10% saying they do so every day. A further 12% use public hotspots at least once a week, with 25% connecting to a public hotspot once in a while.

Yet most don't bother to check the security levels on those hotspots: 30% say they never do, with 26% rarely checking. Just 14% always check.

And of course it's when we're out and about that we need to take particular care of our devices – especially when we're using the London Underground: 1 in 4 (26%) of those surveyed lost or had their device stolen on the tube. The Central and District lines are the most common places to lose devices - 25% lost a mobile on either the Central or District lines

Care must also be taken when out drinking: a bar is second spot for losing a mobile phone, with 22% saying they have lost at least one device here, followed by 11% in a café and 8% in a restaurant.

Unsurprisingly, most of those losses were at night: 18% lost a mobile between the hours of 11pm and 6am, with a further 14% losing their mobile between 7.30pm and 11pm. And 18% lost their mobile in a bar, while another 18% had a tablet stolen in a bar.

Laptops tend to go missing at lunchtime: 33% lost a laptop between noon and 2pm. And they tend to go missing on the Jubilee line – 50% were parted from their computer on that Tube line. With 54% of the respondents saying they commute to work, 44% say they lost a device while on the way home from work, with another 22% saying it was stolen on the way to work.

Hacking and evil twins – a qualitative review

"Scared. Worrying. Paranoid. Self-conscious. Cautious. Annoying. Invaded. Criminal. Angry. Distrust."

These are some of the key words used by people who had been told they had unwittingly logged on to an 'evil twin' * wifi hotspot set up by a "white hat" ethical hacker as part of an experiment to see how we feel about the risks of being hacked.

To gain more insight into those feelings, Trend Micro teamed up with Dr Chris Brauer, senior lecturer at the Institute of Management Studies and founder of the Centre for Creative and Social Technologies at Goldsmiths, University of London, and First Base Technologies, to carry out the "white hat" experiment.

A series of "evil twin" wifi hotspots were created in public places in London to see how people behave when they connect to a hotspot. An "evil twin" hotspot is one that masquerades as a legitimate hotspot, but one that is being run by a hacker to entice the unsuspecting to connect to it so that data such as passwords and banking details can be stolen.

Dr Brauer subsequently spoke to 10 of the participants to gather data on the social and psychological impact associated with increased awareness and potential of rogue wifi networks in public spaces.

Dr Brauer identified eight key points from the study:

- **Public spaces:** the potential presence of rogue wifi points meant that participants felt an increased lack of trust in their physical environments, which were a café and a park in the study.
- **Education:** none of those who took part in the trial knew about "evil twin" hotspots before, nor that they could be used to skim data from those connecting to them.
- **Human dignity:** discovering that they could be hacked while connecting to what they thought was an innocent hotspot made the participants feel that their dignity was injured or compromised by fears associated with knowing that rogue networks were potentially available for them to connect to.
- **Civil rules:** the participants felt that the expansion of digital and social networks endangered social norms and rules of civility, privacy and accountability, which are shifting.

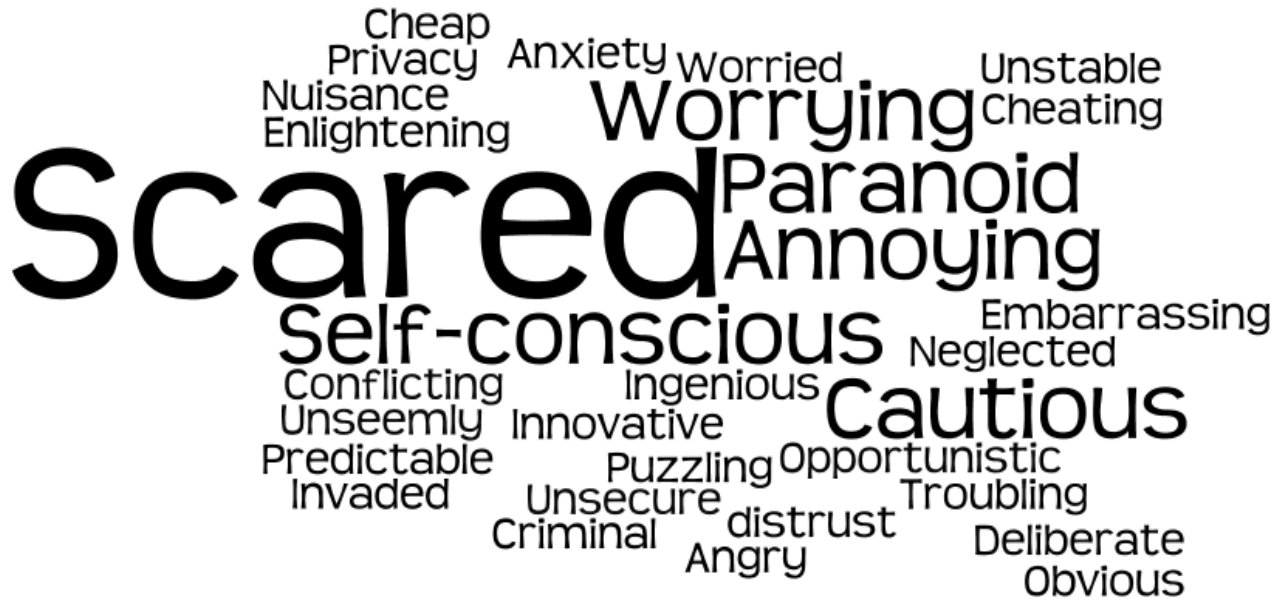
*This 'evil twin' experiment was just a simulation to illustrate one of the many ways people can have their data compromised. All participants were informed of the experiment and gave their full consent to take part.

- **Liability:** the participants were concerned about their liability for other people's data, saying that they felt personally responsible if email were compromised as it would hit the privacy and security of others. They were concerned that they might be held responsible, especially when it came to corporate data such as intellectual property and company secrets. They felt more worried for other people's data than for their own.

- **Opportunism:** despite the risks of such behaviour, seven out of the 10 participants said they had hopped on to an unsecured wifi connection rather than paying to access another network.

- **Priorities:** the participants said that their greatest fears about compromised data were for their bank details, followed by company secrets, email log-in details and intimate photographs or communications.

- **Emotions:** each participant was asked to quickly provide four words to describe how they felt about the experience of participating in the experiment or how they felt about what they now knew about the risks of joining an "evil twin" network. The following is a word cloud of the 40 total responses from the 10 participants:



Conclusion – how can we protect ourselves?

There are a few steps that can be taken to prevent data being stolen via public wifi hotspots, says Rik Ferguson.

- The key step you can take is to make sure your connection to a website is encrypted: “Look for https:// at the beginning of a URL – that s stands for ‘secure’,” says Ferguson. Most browsers display a padlock icon next to the URL for added reassurance.

- If you’re connecting to webmail, make sure that connection is also encrypted. “Hackers are looking for usernames and passwords transmitted in the clear,” warns Ferguson. He adds: “Most ISPs don’t offer an encrypted connection to email unless you ask them to. So you need to be vigilant if you’re on a shared network.”

- Don’t enable shares on your computer when you join a public network. “If you join a network, you’ve obviously opened weaknesses on your machine,” says Ferguson.

- IT departments should consider very carefully what devices they let connect to the network. “They should at the very least identify which devices connect and quarantine those that are not secure enough,” says Ferguson. “That’s only going to get worse with the growth of wearable tech – all of those devices are going to want to connect to the network.”

- IT departments should provide a VPN – virtual private network – to create a secure connection to enterprise networks. “Most employers will provide a VPN,” says Ferguson.

- IT departments should not allow split tunnelling. “That means they’re some traffic to connect directly to the internet and only routing corporate traffic via the VPN. All network traffic on a corporate network should go via a VPN.”

There's a worrying culture of carelessness when it comes to how we look after our devices and our data when we're away from our trusted networks. Says Ferguson: "The survey reveals a worrying attitude of negligence towards work devices and an ignorance of the full impact of losing data without the correct security measures being put in place. Businesses need to ensure they're educating their employees on the secure use of mobile devices to prevent sensitive data falling into the wrong hands that could compromise a company financially.

"Caution must be exercised when travelling on public transport and work trips, and passwords and encryption must be put in place to protect data.

"It's important that employees take the same amount of care with their work device as they do with their personal ones, and are fully aware of the procedures and risks before a device is given to them."

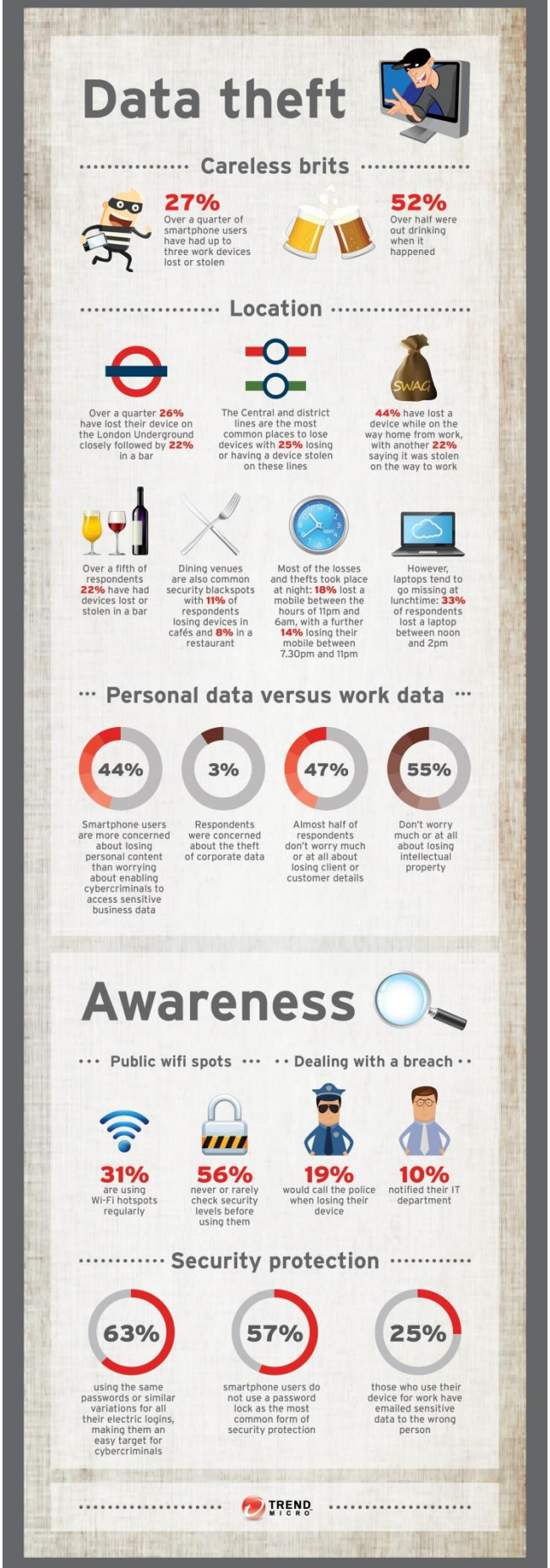
"There are a number of UK and European laws that govern corporate liability for data breaches and fines for leaked customer data can be as high as £500,000. Additionally, new EU regulations are set to increase corporate obligations to notify authorities about data breaches as well as raising fines to 1 million Euros or two per cent of annual turnover," said Vinod Bange, partner at international law firm Taylor Wessing.

"The results from this survey demonstrate that education is required to help employees understand the importance of protecting corporate data on mobile devices and notifying their employer should a breach occur. Organisations that are unaware of data breaches will fail to take the right steps to manage the situation which will diminish their ability to protect customers and avoid monetary penalties or contractual claims from third parties."

Matthew Webb, Head of Technology at insurer Hiscox UK, commented: "Cybercriminals are increasingly targeting mobile devices in the hope of stealing the owner's bank details, but walking away with a wealth of confidential business information can prove even more valuable on the black market. There are several things that employers can do to help safeguard against this risk though, such as encouraging employees to use a login on their mobile device that is at least the same security strength as their work computer, and to change it regularly.

"It is also much simpler for an organisation if employees all work off the same types of devices, so that only security and operating system updates for that one particular manufacturer must be applied. These must be kept up-to-date as well."

Data infographic



Infographic illustrating the key stats regarding awareness of mobile device security and theft. Based on a poll of 2,500 adults throughout the UK, conducted in partnership with Vision Critical.

About the research

Quantitative Research Methodology
The survey was conducted in partnership with Vision Critical of 2,500 adults throughout the UK. Goldsmiths at the University of London also conducted a qualitative experiment with an ethical hacker at First Base to 'pressure test' busy commuter spots in Central London, identifying the ease at which mobile devices can be hacked for their data. For more information please contact trendmicro@3-monkeys.co.uk

Qualitative Research Background
On 17 September, Dr Chris Brauer, Senior Lecturer in the Institute of Management Studies and Founder of the Centre for Creative and Social Technologies (CAST) at Goldsmiths, University of London, conducted a rapid participant observation research project commissioned by Trend Micro in association with a series of rogue Wi-Fi network experiments conducted by First Base Technologies and 3 Monkeys Communications at two public locations in central London.

Over a period of six hours Dr Brauer conducted in-depth interviews with 10 participants in the experiments to gather data on the social and psychological impact associated with increased awareness of the realities and potentials of rogue Wi-Fi networks in public spaces. These participants were either directly involved in the experiments or engaging with network services in the experiment locations. Participants were then contacted 24 hours later to get further feedback following a period of reflection.

About First Base
First Base Technologies LLP provides vendor-neutral testing and security audit services since 1989, including hardware, operating systems, communications and applications. Its approach combines ethical hacking techniques and commercial vulnerability scanning, tailoring results to the specific organisation. First Base also provides post-testing meetings to give guidance for remediation and schedule re-tests.

About Trend Micro
Trend Micro Incorporated (TYO: 4704), a global leader in security software, strives to make the world safe for exchanging digital information. Our solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. Trend Micro enables the smart protection of information, with innovative security technology that is simple to deploy and manage, and fits an evolving ecosystem. Leveraging these solutions, organizations can protect their end users, their evolving data center and cloud resources, and their information threatened by sophisticated targeted attacks.

All of solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe.

For more information, visit www.trendmicro.com. Or follow our news on Twitter at @TrendMicroUK.

Contributors

Rik Ferguson, global vice-president of security research at Trend Micro, is one of the leading experts in information security. He is an advisor to the EU Safer Internet Forum, The Information Security Alliance EURIM, a project leader with Europol at the International Cyber Security Prevention Alliance (ICSPA), a director of Get Safe Online, Vice Chair of the Centre for Strategic Cyberspace & Security Science and advisor to various UK government technology forums. In April 2011 Rik was inducted into the Infosecurity Hall of Fame.

Remaining a part of commercial and government projects for Trend Micro, Rik tries to ensure his views and areas of research reflect the security concerns as experienced by enterprises and individuals as they come to grips with new challenges and technologies.

With over seventeen years' experience in information security, Rik has been with Trend Micro since 2007. Prior to assuming his current role he served as Security Infrastructure Specialist at EDS where he led the security design work for government projects related to justice and law enforcement and as Senior Product Engineer at McAfee focused on network security, intrusion prevention, encryption and content filtering.

Dr. Chris Brauer, Co-Director of CAST, Goldsmiths College, is Senior Lecturer in the Institute for
Management Studies and the spirit behind the CAST initiative. He works with emergent technologies at the intersections of media, social science and computing.

Peter Wood, Chief Executive Officer of First Base Technologies, has worked in the electronics and computer industries for over forty years and founded First Base in 1989. He is a world-renowned security evangelist, speaking at conferences and seminars on ethical hacking and social engineering. He has appeared in documentaries and provided commentary on security issues for TV and radio and written many articles on a variety of security topics. Pete has hands-on involvement in the firm, conducting penetration tests, social engineering exercises and security training. In his spare time he composes and performs club music (as Ghostbrain), drives his heavily modified track-day car as often as he can afford, and shares a geeky science fiction obsession with his wife Didi.

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice. Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Trend Micro Incorporated, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For more information, visit www.trendmicro.com.

©2013 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Securing Your Journey to the Cloud