aruba NETWORKS

Securing #GenMobile: Is Your Business Running the Risk?

REPORT CONTENTS

FOREWORD

"It is becoming increasingly apparent that, particularly with the mainstream adoption of powerful mobile computing, that there is a blurring between the workplace and social life. As such, companies need to be mindful that Information Assurance needs to extend beyond their own equipment to consider, through audits, policies and training, how their employees use of mobile and social technology might create risk for their organisations and potentially introduce new facets to what we understand as digital risk, such as reputational harm. This report contains a wealth of information around these issues and highlights the need for companies to be aware of emerging risks introduced through mobile tech, and ensure they develop a "mobile aware" culture in their organisations."

Professor Andy Phippen,
Professor of Social Responsibility In Social IT
Plymouth University

EXECUTIVE SUMMARY

The new and rising mobile generation - #GenMobile - is a flexible, transparent and collaborative presence in your workforce. For the on-going creativity and growth of your business, this is good news. But for the security of company data and IT systems, there may be cause for concern.

Our global study and report "Securing #GenMobile: Is Your Business Running the Risk?" finds businesses are actually ill- prepared for the high-risk, security-indifferent mind-set of the #GenMobile workforce, creating alarming disparity in security practices around the corporate world.

Particularly, we find these attitudes have created significant discrepancies between industries, individuals and countries when it comes to the treatment of mobile devices and data.

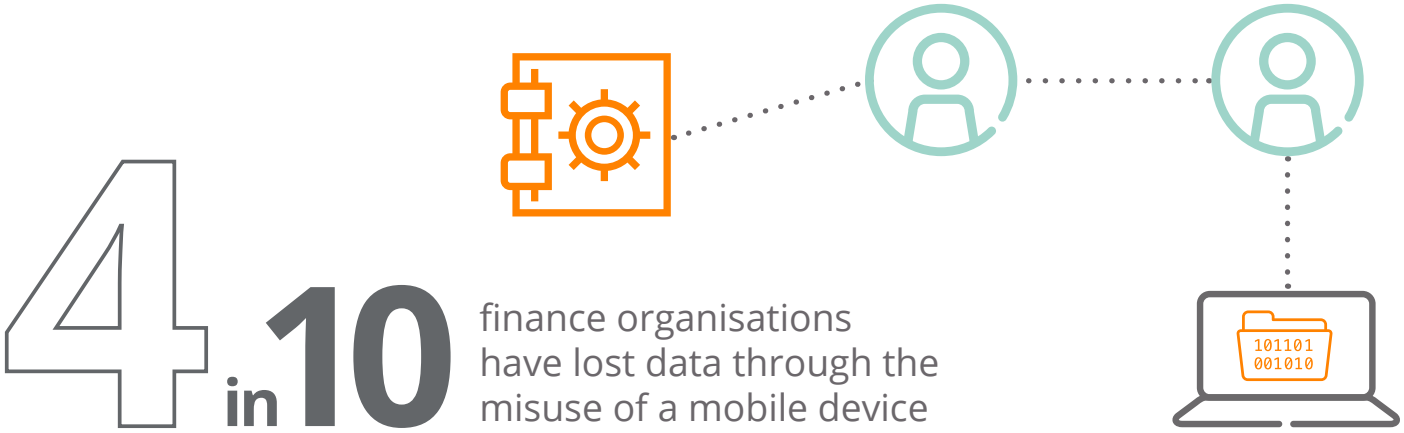
In the culture of sharing, openness and risk that #GenMobile has established, businesses must embrace the inherent drive of these workers to succeed, while ensuring company assets do not suffer as a result.

This research report was commissioned to better understand the pro-risk effect that #GenMobile is having on global business and corporate security, determine where risk is highest, and explain how to understand, embrace and manage the collaborative and innovative behaviour of #GenMobile, while minimizing security risks.

KEY FINDINGS

Our study of over 11,500 employees in 23 countries showed that #GenMobile's willingness to share extends to corporate devices and that they are somewhat indifferent to the importance of security procedures.

- #GenMobile is a workforce of sharers with a general disregard for security procedures: 6 out of 10 are happy to let others regularly use their work and personal smartphones.
- #GenMobile is lax when it comes to security considerations: nearly a third of workers admit to having lost data due to the misuse of a mobile device.
- #GenMobile employees will willingly break the rules if they feel it serves a greater purpose: over half of them would disobey their boss in order to get their job done.



These attitudes represent a fundamental threat to the stability and integrity of corporate IT systems and this report unveils the individuals, industries and countries where this threat is most prevalent today.

The study will also demonstrate that the culture of risk can be mitigated. With the Aruba Networks "Securing #GenMobile: Is Your Business Running the Risk?" online assessment tool, organizations can measure their own risk barometer and benchmark themselves against other organizations in their country and industry. Aruba provides guidance and steps to ensure that IT organisations are successfully prepared for the impact of #GenMobile employees, while embracing their collaborative and innovative attitudes, and protecting the security of corporate data and assets.

RISK AVERSE VS. AT-RISK

As we highlighted in the 2014 Workplace Futures Report, the #GenMobile workforce is instigating a culture of sharing in the workplace: sharing ideas, workspaces, devices and information in all formats, shapes and sizes.

In the last 50 years, the opportunities for businesses to grow have increased exponentially through technology, but at the same time the dangers of cyber security have grown at what is arguably an equal rate. As #GenMobile becomes a more central part of every workforce, businesses need to understand how to manage workplace productivity and morale, without endangering company security.

The reality is that most established firms operate with a generally risk-averse approach inside their chosen market, maybe offset by the needs of a new business unit or sales development division. In contrast, in the #GenMobile universe, risk-averse is considered "the way things used to be done". Today, risk-tolerance (or at least a risk-neutral stance) will usually prevail.

DETECTING RISKY EMPLOYEES

In terms of how company data is treated, the research finds a huge disparity exists between different segments of the workforce.

While all #GenMobile employees appear to share a spirit of risk, the extent to which this affects corporate security depends on the age, sex and salary of the employee. Young, male employees tend to be riskier, but those commanding a higher salary within an organization – regardless of gender – also present cause for concern.

KEY EMPLOYEE FINDINGS:

- Males more prone to data theft: Men are 20% more likely than women to have lost personal or client data due to the misuse of a smartphone, and 40% more likely than females to fall victim to identity theft.
- Younger employees wreak havoc on company security: Respondents over the age of 55 are half as likely to experience identity theft or loss of personal/client data compared to younger employees. The age bracket with the highest propensity of data and identity theft are employees between 25-34 years old. Larger salaries linked to greater security risk: Employees earning more than $60K are more than twice as likely as employees earning less than $18K to have lost company financial data and 20% more likely to lose personal data due to misuse or theft of a mobile device. Ironically, when offered money, those that earn greater than $75K were three times as likely to give out their device password as respondents making less than $18K.

Men are

20%

more likely to lose work data

TRANSPARENCY, OPENNESS AND RISK

The acceptable threshold for risk varies greatly depending on industry. However, #GenMobile demonstrates a much higher willingness to exhibit behavior that is prone to risk than is usually deemed acceptable by their employers. On the positive side, this risk means #GenMobile leans toward a culture of transparency and openness.

Whether this is fueled by the exuberance of well-connected users or a general impatience for growth and development, there is a high-level responsibility to capture and manage this energy using a different security approach -- all without stifling the original business objective.

It may be time to "run the risk associated with mobility", but at the same time, companies and their IT departments need to be smarter about managing this behavior of sharing without sacrificing the security of corporate data and information.

SECURITY RISK THROUGH THE DECADES

EIGHTIES

In the eighties, we saw more essential services move online as email started to take hold and some rudimentary online banking functions emerged. Famous hacks include the Morris Worm, the first DDOS attack, in 1988. Also in this period, a U.S. university student infected 6,000 networked PCs and the "Legion of Doom" hacker group emerged. People started to hear the term cyber security and began to realise that electronic information sharing came with a degree of risk.

NINETIES

- The nineties brought a notable shift to being online. Although serious broadband penetration was still something of a dream, users became comfortable with an online existence where many of the activities they had

previously only considered possible in the physical world could be replicated (and in many cases improved upon) when online. The rise of e-commerce and electronic shopping started during this period and therefore, a commensurate increase in hacks and the proliferation of malware occurred. The "it won't happen to me" notion proved wrong in so many instances that sales of anti-virus software reached an all-time high.

NAUGHTIES

In the so-termed "naughties" between 2000 and 2009, we saw mobile go mainstream. The proliferation and growth of mobile devices was fuelled year-on-year by manufacturers continuously improving processing power, memory, battery life and screen size. However, this was also the era of the ILOVEYOU worm, which spread from the Philippines through corporate email systems and affected as many as 10% of the world's computers causing over $20 billion of damage. Always online and always in your pocket or palm started to mean always at risk.

2010S

So now to the 2010s -- an epoch without a catchy decade-specific name, but a period when we know that #GenMobile arrived. The digital native #GenMobile user outpaces his or her older counterparts in terms of time spent online and time spent connected to other users' information streams. While the force of #GenMobile individuals is felt predominantly within the 18-35 age group, the propensity for users in their 40s and beyond to behave like #GenMobile is also now amplified. As the Royal College of Art's Jeremy Myerson said in Aruba Networks' 2014 Workplace Futures Report, "The contemporary information worker labors in a 'factory' where the gates never close and with work continuously and tantalizingly close to hand around the clock." As we know, this period of connected workers has seen the emergence of online file sharing both in and out of work, Edward Snowden's famous data leaks, which show employees themselves present a serious corporate threat, and a Bitcoin exchange that was declared bankrupt after losing $460m to hackers.

Over a

third

of businesses don't have any type of basic mobile security policy in place

SHARING BECOMES THE NORM

Today's array of connected devices and applications has put instant information retrieval in the palm of our hands. Combine with the ability to seek peer affirmation and opinion from a trusted group of social contacts and, suddenly, you have #GenMobile in a position where they feel empowered and emboldened to conquer the world.

The fear factors harboured among members of the workforce who have witnessed the initial rise of harmful security breaches are less present in #GenMobile. This study suggests that we're in a period of collaborative experimentation with 6 out of 10 individuals being happy to let others regularly (at least once a month) use their work smartphones.

Perhaps more worrisome to IT, nearly a fifth of employees do not have passwords on their mobile devices. When asked why they chose not to secure their mobile devices, 22% said because it was easier to share their device with others.

SECURITY INDIFFERENT ATTITUDES RISE

#GenMobile workers believe this openness is not an information security risk, but what they call "collaborative sharing". This represents a different operational, as well as risk, mind-set.

The survey found that over half (51%) of people surveyed think using mobile apps can drive more productivity and another 48% believe it gives their company a competitive edge, suggesting that the #GenMobile approach brings business benefits. and potentially bigger profit margins. But while many of these workers are keen to take advantage of the benefits of mobility, not all are prepared to use the latest tools to protect themselves or the company. Well-established security technologies like Virtual Private Networks (VPNs) were only used by 58% of remote employees.

With an increasing proportion of work undertaken while outside of office and the protection of a corporate firewall or a Virtual Private Network (VPN), flexibility is high but so to are the risks. Once again, this can be a positive, but a corollary level of security controls are needed to bring balance.

Looking again at #GenMobile behaviour: seven in ten (70%) say they have or would consider revealing the passwords to their work devices. Another 5% revealed their work device password because they were offered money to do so.

Over one-third of respondents use their devices for both work and leisure and one in five don't even consider security when buying devices. This leads to a degree of vulnerability in company security as demonstrated by the fact that 31% of respondents were found to have lost data due to the misuse of a mobile device.

#GenMobile attitudes can be compared to driving at high speed with some very creative twists and turns, but often means doing so without a seatbelt.

THE INDUSTRY RISK LANDSCAPE

Our research also compared the levels of risk taken by various industries. While the physical size of each industry differs from country to country, device usage trends are consistent enough to paint a clear picture.

The findings suggest a higher propensity for risk within the industries where technology is most widely used. At the same time, there is a lower propensity for risk within the industries where not only is there less technology, but more policy regulation controls in place governing its usage.

High tech employees are nearly

two times

more likely than hospitality or education workers to simply give up their device password if asked for it by IT

KEY INDUSTRY FINDINGS:

- Finance is leaking data: Believe it or not, 39% of respondents from financial institutions admit to losing company data through the misuse of a mobile device, which is 25% higher than the average across all industries surveyed. The public sector (excluding education) is the least likely to report lost or stolen data.
- High tech is at high risk: High tech employees are nearly two times (46%) more likely than hospitality or education workers to simply give up their device password if asked for it by IT.
- Teachers need a lesson on security: The study reveals that educators are 28% more likely to store passwords on a sheet of paper compared to those in high tech. Educators also score the lowest compared to all other industries when asked if they password-protected their personal smartphones.

SELF-EMPOWERMENT SUCCEEDS

With over half (56%) of employees willing to disobey their boss to get something done, and over three quarters (77%) willing to perform self-service IT, #GenMobile displays its willingness to go it alone.

A culture of self-empowerment has emerged, seemingly fuelled by a high level of inherent trust that IT systems and data are being adequately secured. Almost 9 in 10 #GenMobile employees believe that the security provided by their IT department is mostly adequate. Furthermore, 8 in 10 trust IT with a large part of their personal data.

However, do these attitudes reflect the reality of IT security readiness? Or is this simply proof that #GenMobile is less concerned than ever about security and simply prepared to run the risk in order to have the self-empowerment they desire?

Over half (51%) of IT departments do not recommend a specific mobile device to use for work purposes. Firms can go all the way and offer a Choose Your Own Device (CYOD) option for users or they can test devices to ensure they meet basic security and wireless requirements. Not vetting devices is a missed opportunity to shore up threats and reduce help desk calls before they happen.

Over

half

of workers today said they are willing to disobey their boss to get something done

The research suggests a higher predisposition towards at-risk behavior among workers in what may be described as economically emergent countries. The growth in these developing, fast-firing countries is apparently unbridled at times, and appears to owe an intrinsic cause-and-effect debt to this mindset. While more developed countries exhibited employee behaviors the represented less risk, there is still cause for concern as IT must continually evolve to be prepared for emerging threats.

GLOBAL RISK FINDINGS

Our research study has identified by country the workers that are most at risk based on embracing Mobility.

THE GLOBAL DIFFERENCE

Top 5 Risk-Averse Regions

Sweden
USA
Canada
UK
Norway

Top 5 At-Risk Regions

Malaysia
Thailand
S. Korea
China
UAE

*An 'At-Risk' attitude has been defined in this study by those who are most likely to express a distrust towards their IT teams, admit to disobeying bosses in order to complete tasks, have lost company data due to the misuse of a mobile, use the fewest amount of passwords to protect devices, are most likely to use jail-broken devices and are most likely to agree with the statement 'The adoption of mobile apps in my organization will give us a competitive edge'.

WHAT SHOULD YOU DO TO LOWER YOUR RISK?

Start by understanding your risk levels relative to those in your country and industry by taking the Aruba Networks "Running the Risk: Secure Mobility Risk Index". This tool will provide a benchmark of how your mobile security risk levels compare to other companies in your country and sector. Secondly, firms should adopt the following five-step checklist to ensure their IT organizations are prepared for the risks that #GenMobile workers are bringing into the enterprise and are staying ahead of these emerging trends:

1. A basic security policy is an absolute prerequisite for every firm to lay down a description of its core protection controls and its employees' usage of those technologies. Even for a small firm of just two employees, formalizing an approach to information security is crucial. Such a policy should cover roles, devices, locations and other contextual attributes.

2. Organizations should implement enforcement rules that extend from applications to devices to the network. Such an approach should integrate services across MDM, firewalls, IPS and policy engines to deliver common policy enforcement for all sensitive information.

3. IT must measure and monitor user behavior to ensure that security policies are mapped to business objectives. This will ensure that policies achieve the result of securing corporate information and systems without impacting usability and employee productivity.

4. Even the most well thought through security frameworks will fail without the requisite employee training. This should not only include a needs-assessment by employee type, but should also educate employees on why such actions are important and how they can assist in improving corporate security.

5. Finally, ensure that IT has a mechanism for employee feedback and a service level agreement in place for how to respond to employee input and requests. Often times IT is able to improve the effectiveness of automated workflows and security policies simply by listening to employee feedback.

51%

say that mobile technologies enable them to be more productive and engaged

Respondents over the age of 55 are

half as likely

to experience identity theft or loss of personal/client data compared to younger employees

CONCLUSION

#GenMobile is the future of business -- and that means every business. Old business models that fail to adapt to #GenMobile will slowly crumble and may ultimately not survive. The arrival of the always-on, mobile-office and #GenMobile employee is as tangible and impactful a sea change on industry as the arrival of the Internet itself.

In a contemporary, connected world, firms need to nurture creativity, while at the same time minimize the risk of data and information loss. As a result, employers need to take an adaptive trust approach to connectivity and data security. Identifying individual worker preferences that factor in multiple layers of contextual information in order to build secure infrastructures around them is a baseline requirement.

How the business world now adapts to the behavior of the #GenMobile workforce may be the make or break for long term boom or bust. Embracing #GenMobile's penchant for openness, innovation, collaboration and some degree of risk is good – but only when an organization can understand and plan for the security risks these behaviors bring with them.

For more information on the latest in Secure Mobility solutions or on implementing a Secure Mobility strategy for #GenMobile, visit **www.arubanetworks.com** or contact your regional Aruba Networks representative or authorized partner.

The age bracket with the highest propensity of data and identity theft are employees between

25-34

years old