# Contents

Executive summary ............................................................................................................................................. 3  
Key observations ............................................................................................................................................... 4  
About the survey ............................................................................................................................................. 5  
Key findings – the numbers ......................................................................................................................... 6  
Snapshot view .................................................................................................................................................. 7  
1. Information security .................................................................................................................................. 8  
   1.1 Understanding the information security function ............................................................................. 8  
   1.2 Effectiveness of this function ........................................................................................................... 9  
   1.3 Plans for expansion .......................................................................................................................... 10  
   1.4 Challenges faced ................................................................................................................................ 10  
2. Mobile devices and emerging technologies .............................................................................................. 12  
3. Motivation for information security ......................................................................................................... 14  
4. Incidents ..................................................................................................................................................... 15  
   4.1 Occurrences ......................................................................................................................................... 15  
   4.2 The causes of an information security breach ................................................................................. 16  
   4.3 The cost .............................................................................................................................................. 16  
   4.4 A proactive approach ....................................................................................................................... 18  
5. Overall assessment .................................................................................................................................... 20  
Protecting your organisation ....................................................................................................................... 21
Now in its second year, this survey has all the hallmark areas which the inaugural survey focused upon but has also explored additional areas including cloud computing, BYOD and regulatory compliance.

Laws and regulations, coupled with the growing need to protect personal, intellectual and proprietary information as well as the reputation of an organisation have reinforced and enhanced the need for investment in information security. Unfortunately, information security is still a long way from integrating with the strategy and objectives of an organisation as evidenced by the increase in the average cost of a large cybercrime incident at €135,000 per incident, as well as the increase in the number of respondents who feel that appropriate measures are not in place to detect incidents of cybercrime in their organisation. In terms of remediation and clean-up costs associated with the incidents experienced by respondents’ organisations, the average cost stood at €29,954 per incident.

A new addition to the 2013 survey was to quantify the financial impact and total cost of cybercrime to businesses in Ireland. On average, instances of cybercrime cost 2.7% of annual turnover. Of most concern perhaps is the 15% of respondents who stated that cybercrime costs more than 10% of their annual turnover. These figures clearly illustrate the impact on Irish organisations as a result of cybercrime, and, more importantly, the lack of proactive planning and defending against such threats.

Of the respondents who experienced serious incidents, 14% reported losses above €250,000 per incident. 67% of respondents indicated that their organisation had not looked at cyber insurance or risk transfer as a mechanism to cover against cyber attacks, business interruptions or data theft/loss. These findings reinforce the need to proactively identify incidents and to keep up with technology advancements as only 40% of serious incidents were identified proactively.

Furthermore, it emphasises that organisations need to strengthen their procedural controls and obtain signed acceptance and adherence to the organisation’s security policies as the survey indicated that only 55% are currently doing so. Whilst this represents an increase from last year, it is still far below industry best practices and could expose organisations to various internal incidents, as well as potential legal implications should they look to prosecute, or dismiss employees or third party personnel.

A well-received addition to this year’s survey was the topic of cloud computing. While 60% of respondents indicated that their organisation uses cloud based services in some form, 39% of the respondents believe that privacy and data protection was the single biggest risk associated with the cloud, and continued to be a barrier for the use of cloud based services and solutions.

A proactive approach to cybercrime is important for organisations to ensure undetected incidents do not cause exponentially greater damage over a sustained or extended period of time. 45% of respondents believe their organisation proactively identified just over 40% of serious incidents, an alarming drop from 58% in 2012. Additionally 44% of respondents regard their information security policy as proactive while 47% consider their policies reactive.

We hope you find this report insightful in benchmarking your organisation’s effort against the ever increasing threat of cybercrime.

Colm McDonnell,
Partner, Enterprise Risk Services, Deloitte
Organisational strategic awareness and alignment

Information security is best integrated into the culture of an organisation if the board and senior management are aware of their responsibilities and actively support the process. The survey findings indicated that only 42% of respondents felt that information security is very well understood by the board with 33% of the respondents stating that information security efforts were well aligned with the organisation’s overall strategy.

Organisational drivers for information security

42% of respondents indicated that satisfying regulatory requirements was the main driver for investment in information security from senior stakeholders.

Protecting the reputation of the organisation came second, with 28% of survey respondents indicating that brand/reputation protection was the main driver for investment in information security. Interestingly, none of the respondents indicated investing in information security to gain an edge over competitors.

Mobile and smart devices

Of particular interest was the approach taken towards smartphones and bring your own device (BYOD), where 50% of organisations stated they only support corporate provided devices, with 29% supporting both corporate and employee purchased devices.

Given the escalating malware and attacks targeting smartphone devices, of concern was the 31% of organisations that had no additional security measures deployed on mobile devices (such as encryption, mobile device management solutions, etc.), despite corporate information being stored/processed on the mobile devices.

Response to cybercrime and information security breaches

Preparation, and identification of, in addition to responding to incidents are of particular concern to respondents. Results show that only 44% of respondents believe that their organisation proactively identifies incidents and over 40% of the serious incidents encountered were identified proactively. The most common method of breaching security in an organisation is due to hacking, as identified by 19% of respondents.

The survey findings also indicate that 21% of respondents feel that keeping up with technology advancements is the top security initiative for 2013 while only 7% stated that regulatory and legislative compliance is a top initiative for 2013.

40% of respondents stated that their organisation had experienced at least one security breach that they know of in the past 12 months.

Resourcing and internal challenges

The demand for information security professionals continues to grow, with 44% of respondents stating that they are either currently recruiting or plan on taking on additional information security staff over the next one to two years.

42% of respondents felt that current funding for security was adequate, with a further 44% stating that funding was limited, thus impacting on their ability to prevent cyber attacks, or breaches of security.

Just 16% of respondents saw up-skilling existing security personnel as a top initiative.
Deloitte, in association with EMC, presents the second annual Irish Information Security and Cybercrime Survey. This survey was conducted in the second quarter of 2013. Respondents included information security leaders of multinationals, Irish organisations and subsidiaries. These organisations operate across a range of industries including financial services, public sector, manufacturing, IT, semi-state and insurance.

**Figure 1 - Primary function of the organisation surveyed**

- Financial services: 21%
- IT (hardware/software): 9%
- Education: 9%
- Government: 7%
- Telecoms/ISP: 7%
- Manufacturing: 5%
- Semi-state: 2%
- Professional services/consultancy: 5%
- Healthcare: 5%
- Pharmaceuticals: 2%
- Food products/beverages: 2%
- Transport: 5%
- Insurance: 5%
- Legal firm: 2%
- Other: 5%

**Figure 2 - Size of organisation surveyed, in terms of turnover (or annual budget for public sector organisations)**

- < €5 million: 44%
- €5 - €25 million: 12%
- €25 - €100 million: 7%
- €100 - €250 million: 5%
- €250 - €500 million: 11%
- €501 million - €1 billion or more: 5%
- Other: 21%
Key findings – the numbers

€135k is the average cost per organisation for a security incident over the past year.

2.7% Cybercrime costs Irish organisations on average 2.7% of their annual turnover.

€29,954 was the average clean-up and remediation cost to organisations following an incident.

49% of respondents rate their organisations’ overall readiness to deal with cybercrime incidents as fair or poor.

67% of respondents have not looked into cyber insurance.

63% of respondents believe their organisation is only partially equipped, or do not consider their organisation to have adequate measures to deal with cybercrime.

57% of respondents stated that no further actions were taken following an investigation of internal or external incidents.

30% of respondents believe that evolving technical threats present the biggest challenges in information security.

76% are of the view that existing policies only partially address or fail to address recent business and technology changes (BYOD, cloud).

BIGGEST DRIVER The biggest driver for information security investment/sponsorship is meeting regulatory requirements.

33% believe measures to detect incidents of cybercrime are either not appropriate or not adequate.
The table below illustrates changes in key statistics from last year’s report.

<table>
<thead>
<tr>
<th>Survey 2012</th>
<th>Survey 2013</th>
<th>Increase/Decrease (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage of respondents that detected or are aware of breaches in the past 12 months</td>
<td>46%</td>
<td>40%</td>
</tr>
<tr>
<td>Respondents planning on recruiting additional personnel for the information security function</td>
<td>24%</td>
<td>44%</td>
</tr>
<tr>
<td>Respondents who feel that appropriate measures are not in place to detect incidents of cybercrime in their organisation</td>
<td>3%</td>
<td>23%</td>
</tr>
<tr>
<td>Percentage of serious security incidents identified proactively</td>
<td>58%</td>
<td>40%</td>
</tr>
</tbody>
</table>

Security breaches are becoming more common, and information security leaders feel that the resources that they are currently working with are not sufficient to deal with the rise of cybercrime threats.
1.1 Understanding the information security function

Our results show that there is a good level of understanding of information security risks at executive and board level. 42% of those surveyed believed that the executives and boards of their organisations understood these risks and impacts very well or better. 14% of respondents highlighted that they believe that these risks are not well understood. This relatively high level of awareness of the associated risks could be attributed to recent increases in cybercrime, as well as numerous high profile cases.

With this level of understanding in mind, organisations should ideally have their information security efforts aligned with the organisation’s overall risk management programmes. However, the results show there is room for improvement when it comes to aligning the information security risk and the overall business risk. Just 33% of respondents said that their information security efforts were well aligned with the organisation’s overall risk assessment or risk management programme. Although 46% of respondents believe that the security efforts and overall risk assessment were somewhat aligned - just under half of organisations are seeing some success in this department - the majority of organisations should be better aligned with business risk in order to reduce duplication of efforts and costs.
1.2 Effectiveness of the information security function

A large majority (65%) of the information security professionals surveyed believe that their organisations’ information security activities are good or very effective. 21% consider their security activities as average and predominantly reactive. While most respondents consider their respective organisations to be adequately protected, merely 7% consider themselves to be very effective.

A similar picture was painted when respondents were asked to describe their security monitoring strategy. A smaller, but still notable proportion of respondents (44%), stated that their security monitoring strategy is proactive, with a further 47% feeling that their strategy is reactive. This highlights how respondents are relatively satisfied with their security monitoring strategies, but there appears to be room for the information security function to be more proactive than at present.

Figure 5 - In terms of information security effectiveness - how effective do you feel your information security activities are?

<table>
<thead>
<tr>
<th>Description</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very effective</td>
<td>7%</td>
</tr>
<tr>
<td>Good</td>
<td>58%</td>
</tr>
<tr>
<td>Average and predominantly reactive</td>
<td>21%</td>
</tr>
<tr>
<td>Somewhat effective</td>
<td>14%</td>
</tr>
</tbody>
</table>

Figure 6 - Would you describe your security monitoring strategy as mostly proactive or reactive?

<table>
<thead>
<tr>
<th>Strategy</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive</td>
<td>44%</td>
</tr>
<tr>
<td>Reactive</td>
<td>47%</td>
</tr>
<tr>
<td>No security monitoring strategy</td>
<td>9%</td>
</tr>
</tbody>
</table>
1.3 Plans for expansion
When asked about future plans for additional staff in the information security function, 44% of respondents stated that they are either currently recruiting or plan on taking on additional information security staff over the next one to two years. 16% said they did not know if they would be making any additions to the function.

1.4 Challenges faced
Evolving technical threats and attacks were cited by 30% of respondents as the biggest challenge in information security. 24% cited employees and their activities and a further 21% indicated that their organisation is not in a position to perform an adequate review of risks prior to the introduction of new technologies. When compared to results from last year’s survey, the significance of employee activities as a security challenge has reduced considerably, from 50% of respondents to 24%. Respondents are more concerned about keeping pace with threats that are presented by new technologies.
The reduced significance of employees as a security challenge could be linked to the improved levels of policy education among users. 55% of respondents said that all users in their organisation had provided signed acceptance and adherence to the organisation’s security policies, up from 46% last year. While the percentage of organisations that have had employees sign full acceptance of security policies should be higher than 55%, it appears that steps have been taken to address the significant threats that employee activities present.

When asked about the funding received by the information security function to combat threats, 14% believed that there was insufficient or no funding available. 44% stated there was limited funding available.
Respondents were also asked to what extent mobile devices are supported in their organisations. Remote access to company information via mobile devices brings additional challenges and risks. 79% of respondents said their organisation supports the use of corporate provided mobile devices only, with 31% also permitting the use of employee purchased mobile devices – bring your own device (BYOD). These stats were broadly in line with 2012 statistics, illustrating a continued interest and introduction of BYOD within organisations.

Coinciding with the increased demand for network support of mobile devices, many organisations are implementing additional security procedures for mobile devices. 50% of respondents said that their organisation had implemented specialist technologies to increase mobile security with 17% saying that additional in-house mechanisms had been implemented. It is worth noting that 31% of organisations surveyed had no additional security measures; despite corporate information being stored/processed on the mobile devices.
This year respondents were asked to what level cloud services are currently being used within their organisations. For more than half of respondents (53.5%), cloud services appear to have been adopted, albeit mainly on a departmental or specified business units basis. A quarter of respondents (25.5%) stated that while they are not currently using cloud based services, they plan to do so in the next 12 months. Somewhat surprisingly only 7% stated that cloud services are widely used throughout their organisation, and a further 14% stated that they have no plans for cloud services to be used in the short to medium term.

In addition to gauging cloud adoption, our survey looked at the single biggest risk for use of cloud services. Unsurprisingly two fifths of respondents cited privacy and data protection as the number one concern, while a further fifth stated unauthorised data access/disclosure. Of interest, only 9% of respondents cited lack of clarity or reporting, with a further 7% citing the technical security of the cloud environment. In terms of reporting breaches/ clarity/disclosure by the cloud provider, only 7% of respondents cited this as their main concern, perhaps illustrating a perceived level of trust in cloud providers.

Figure 13 - Is your organisation actively using cloud based services?

- No – we also have no plans for use of cloud services in the short to medium term: 14%
- Not at present - but we plan to use cloud services within the next 12 months: 25.5%
- Yes – but currently only a departmental level: 53.5%
- Yes – cloud services are widely used throughout our organisation: 7%

Figure 14 - Which of the following do you consider as the single biggest risk for use of cloud services by your organisation?

- Privacy and data protection concerns: 39.5%
- Data disclosure/unauthorised access to organisational information: 20.9%
- The risk of cyber attack resulting in the unavailability of services: 9.3%
- Vendor "lock-in", or the inability to easily move to an alternate provider: 4.7%
- Lack of clarity around governance and reporting: 9.3%
- Clarity and reporting of incidents/breaches/disclosure by cloud providers: 9.3%
- Technical security concerns related to the cloud environment: 7%
When asked about the motivation behind investment in advanced security technologies and information security in general, one rationale stood out from the others. 45% of respondents said that their primary motivation for the use of advanced security technologies is compliance and reporting.

However, when the respondents were asked about their organisation’s top security initiative for this year, only 7% chose information security, regulatory and legislative compliance, perhaps indicating a shift from traditional motivations. 21% of respondents said that security related to technological advancements was the top security initiative. The second highest initiative was data protection at 19%. This seems to paint the picture that organisations are becoming more concerned with addressing emerging issues caused by new technologies, rather than simply focusing on regulatory compliance and reporting.
This conflicts with the rationale for investment in information security, with 42% of respondents saying that the main reason for investment in information security from senior stakeholders was meeting/satisfying regulatory requirements. There would appear to be a disconnect between traditional motivations for investment in information security and the planned information security initiatives over the short to medium term. Interestingly, none of the respondents indicated that having a competitive edge was a driver for investment in information security.

4. Incidents

4.1 Occurrences

40% of respondents stated that their organisation had experienced at least one security breach, which they know of, in the past 12 months. Over a quarter (28%) are unsure of how many security breaches their organisation experienced in the past 12 months. Of the incidents which have been identified by these organisations, 34% have been identified by existing technologies (including reporting and alerts) in the organisation.
When asked what steps were taken by the organisation following an instance of cybercrime, it is interesting to learn that 26% of respondents said that no follow up actions were taken in light of these incidents. 41% of organisations decided to revise policies/procedures in the wake of instances of cybercrime, while 14% said that incidents lead to their organisation investing in new technologies.

4.2 The causes of an information security breach

The most common method of breaching security in respondents’ organisations was hacking, with 19% citing this as the main cause of security breaches in their organisation. Other common methods of attack included Denial of Service (DoS), Distributed Denial of Service (DDoS) and malware.

4.3 The cost

31% of respondents said that the direct financial impact on the business as a result of their largest incident was more than €100,000. 14% reported losses above €250,000. The survey found that the average cost to organisations of the largest cybercrime incident stood at €135,000. This figure is significantly higher than the average figure from 2012, which stood at €41,875 per incident.
In terms of remediation and clean-up costs associated with the largest incidents experienced by respondents’ organisations, the average cost to organisations stood at €29,954. 24% of respondents indicated that the remediation/clean-up costs for the largest incident their organisation experienced was €50,000 or more.

Following demand from our 2012 survey, we included a mechanism for organisations to benchmark the overall cost of cybercrime. Worringly, the cost of cybercrime to organisations is at 2.7% of annual turnover. Particularly alarming was that 15% of respondents stated that cybercrime costs more than 10% of their annual turnover. 56% of respondents were impacted by 1% or less of turnover, which still represents a sizeable loss for many organisations, and should form a driver for security and risk related activities moving forward.
4.4 A proactive approach

It’s more important than ever that organisations take a proactive approach to protecting themselves from cybercrime. In this year’s survey, 45% of respondents believe that their organisation proactively identified just over 40% of the serious incidents which they encountered, compared to 58% from last year. This is a significant decrease, as breaches that go undetected for extended periods of time can cause exponentially greater levels of damage. The risk remains that a large amount of incidents are not being identified prior to impacting on the business. 33% of respondents believed that less than 10% of incidents encountered by their organisation were proactively identified.

This mind-set of proactively identifying and handling security incidents and cybercrime is broadly reflected in the prioritisation of cybercrime risk in the organisation. 33% of respondents believe that the risk of cybercrime was prioritised in their organisation, while 39% said that no special steps had been taken to address the threat of cybercrime. 7% of organisations said that they did not view cybercrime as a major risk to their organisation. This reflects the overall awareness of the risk of cybercrime today, and shows that organisations need to become more active in educating themselves about cybercrime threats, how they can prevent and respond to these threats and adopt a proactive approach.

Figure 23 - In your estimation, what percentage of serious security incidents are identified proactively within your organisation?

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 50%</td>
<td>33%</td>
</tr>
<tr>
<td>40%-49%</td>
<td>12%</td>
</tr>
<tr>
<td>25%-39%</td>
<td>17%</td>
</tr>
<tr>
<td>10%-24%</td>
<td>5%</td>
</tr>
<tr>
<td>Less than 10%</td>
<td>33%</td>
</tr>
</tbody>
</table>

Figure 24 - Does your organisation identify cybercrime as a major risk to the organisation?

- Preventing cybercrime is a priority: 33%
- Yes, but no special steps have been taken: 28%
- Cybercrime is one of many threats: 21%
- Somewhat: 11%
- No: 7%
Most of the organisations surveyed believe that they are in a decent position to deal with cybercrime incidents as they occur. 51% stated that they are in a good or excellent position to deal with cybercrime incidents, while a further 35% say they have a fair level of readiness to deal with incidents. 14% admit that they are in a poor position to handle security incidents.

Just over one third (37%) have specialist systems and mechanisms in place to detect incidents of cybercrime, 30% of respondents stated that they only partially have appropriate mechanisms in place. 33% of respondents feel that their organisation does not have adequate measures and systems to detect incidents of cybercrime. With cybercrime incidents increasing internationally, these results illustrate the potential challenges facing Irish organisations in the coming years when dealing with cybercrime.
5. Overall assessment

Organisations appear to be relying on internal policies, procedures and resources as the primary mechanism to combat the threat of cybercrime, rather than outsourcing to specialists or acquiring new specialist resources.

The top priorities for improving cybercrime readiness in 2013 are introducing new technical controls or systems (20%), up-skilling existing information security personnel (16%) and introducing new procedures and security standards (15%). Linking with specialist resources and expert providers is on the agenda for only 6% of respondents.

For 2013, the top security initiative for organisations was to introduce new procedures and security standards internally, with one quarter of respondents citing this as their top initiative, along with improving current technical controls at 16%.

Taking into account last year’s findings, there appears to be a preference within organisations to improve existing internal awareness and policies along with developing new internal initiatives. While the ability to deal with threats using internal resources is a very positive attribute, it should also be noted that organisations will need to rely on external specialists and as well as investing in new technical systems to combat cybercrime. In an environment where organisations are always playing catch up against cyber criminals and the threats they pose, these specialist systems and experts are important tools in the continuing fight against cybercrime.

Figure 27 - What resources has your organisation relied on to respond to incidents occurring in 2012?
Cybercrime costs. It costs time, money, resources and, most importantly, it costs reputation. Survey findings show that there are varying degrees of readiness and preparation within Irish organisations in terms of defending against cyber attacks.

In order to reduce the risk of cyber attacks, a planned, proactive and sustained approach is of critical importance.

Four key priorities are critical:

**Prepare**

Prepare for a cyber attack is a business issue, successful attacks directly impact earnings and assets. Although the technical defences must be built by ‘the IT guys’, a breach of those defences can have far reaching business consequences. Identifying the business risks and deciding how and when cyber issues should be escalated are the starting points in developing an effective, coordinated business response.

- Ensure the right governance structure is in place to enhance and maintain preventative and detective security capabilities.
- Implement training and awareness controls and investigate potential alliances based on technology.
- Ensure consistency in practices of information sharing and incident handling across all departments by effective communication and co-ordination.

**Aware**

When threats were relatively slow in developing, organisations could build an effective defense based upon classic detect-and-respond security principles. The speed with which new attacks are now developed, and the complexity of the internet environment, mean that this approach is no longer adequate. Organisations now need to both use dynamic, real-time cyber threat intelligence and to monitor their own vulnerabilities regularly if they are to maintain an effective defence.

- Train and educate users on the use of suitable technical controls so that they are aware of known exploits and attacks.
- Leverage the wealth of threat intelligence that is available to ensure greater awareness of the internal and external threats to your organisation.
- Regularly engage and consult with cyber security leaders to ensure up-to-date cyber threat intelligence.
**Respond**

When a breach occurs the response must be fast, thorough and decisive. Immediate action is required on several fronts. The nature of the breach must be established and the losses and damage understood. Further attacks must be prevented by urgent action, while a longer-term solution is found. Media and external stakeholders must be dealt with. Legal action may be required.

A bad breach response can cause great damage to reputation and shareholder value. It may also heighten the risk of further attacks.

- Outline a clear set of guidelines defining the strategy which should be taken upon combating a breach in security.
- Ensure you have the ability to rapidly respond to an incident in order to limit any adverse impact on your organisation.
- Analyse the anatomy of the cyber attack to determine the root cause and recommend remedial activities and other associated responses.

**Defend**

In order to adequately defend your organisation against successful cyber attacks, continual investment and enhancement of current processes and security components are required. Security is a “point in time” assessment, which needs to be managed and continually developed in order to stay current and up to date with emerging threats and attacks.

- Continue to invest in enhancing and maintaining controls that protect your digital assets against cybercrime.
- Consistently improve the information sharing processes, and where possible automate the controls and practices to deal with the changing cyber security threat landscape.
- Constantly set targets and test systems to ensure ongoing defense.
- Learn from prior incidents or events, and ensure that “lessons learned” continue to drive new practices to further enhance the security capabilities of your organisation.

**Learn more**

At Deloitte, we are committed to supporting CIOs and Information Security Managers against the omnipresent threat of cybercrime attacks. We provide timely and valuable thought leadership to assist them in their role of preventing attacks.

See below for some of our most recent publications:

- 2012 Deloitte – NASCIO Cybersecurity Study
- 2013 TMT Global Security Study
- IT risks and security challenges – Deloitte article series from Wall Street Journal
- 2012 Deloitte Ireland CIO Survey

Identifying the business risks and deciding how and when cyber issues should be escalated are the starting points in developing an effective, coordinated business response.
Information security is still a long way from integrating with the strategy and objectives of an organisation as evidenced by the increase in the average cost of a large cybercrime incident at €135,000 per incident.

Colm McDonnell, Partner, Enterprise Risk Services, Deloitte
For more information on the Deloitte Irish Information Security and Cybercrime Survey, in association with EMC, please contact:

Colm McDonnell  
Partner, Enterprise Risk Services, Deloitte  
T: +353 1 417 2348  
E: cmcdonnell@deloitte.ie

Jared Carstensen  
Manager, Enterprise Risk Services, Deloitte  
T: +353 1 417 5700  
E: jcarstensen@deloitte.ie

Jason Ward  
Director for Ireland, Scotland and UK North, EMC  
T: 1800 932362  
E: SalesIreland@emc.com

About EMC  
EMC Corporation, the IT multinational that employs over 3,000 people in Ireland, is a global leader in enabling businesses and service providers to transform their operations and deliver IT as a service. Fundamental to this transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping IT departments to store, manage, protect and analyse their most valuable asset - information - in a more agile, trusted and cost-efficient way. Additional information about EMC can be found at www.EMC.com

© 2013 Deloitte & Touche. All rights reserved