

SHAREPOINT SECURITY SURVEY BY CRYPTZONE

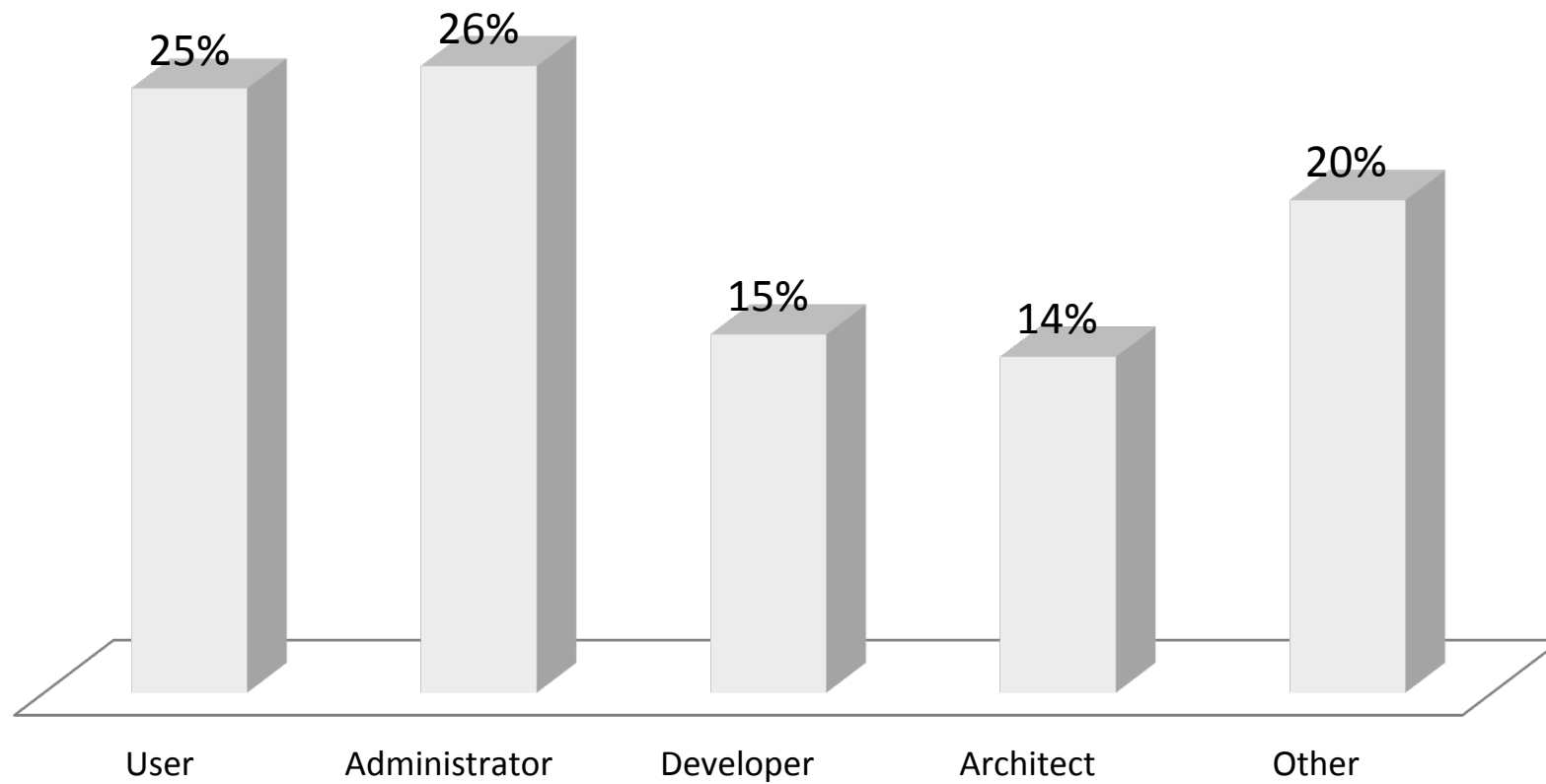
© The Cryptzone Group 2012

Introduction

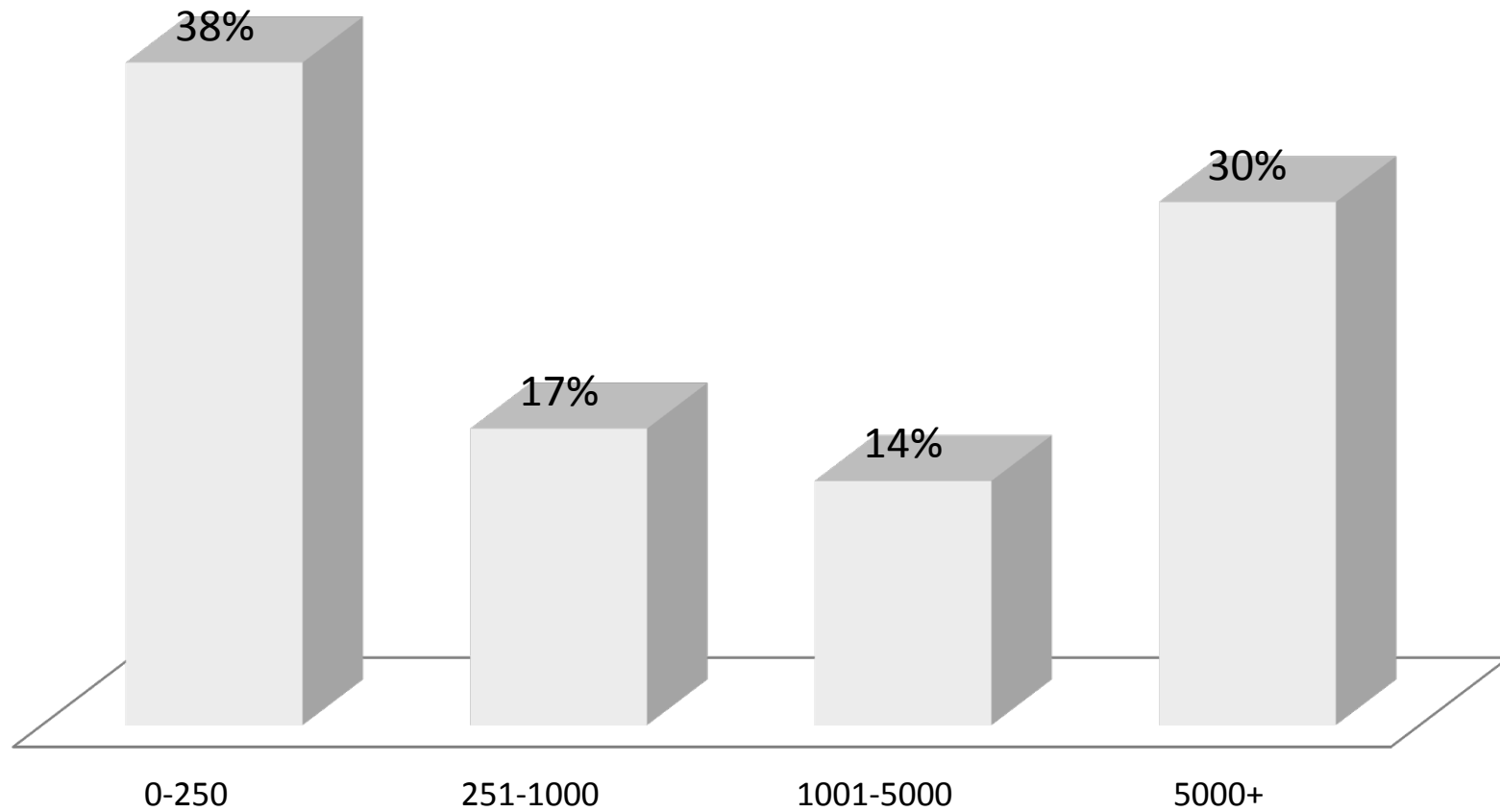


This survey was conducted amongst 100 attendees at the UK SharePoint Saturday conference held in Nottingham, United Kingdom in November 2011. Respondents consisted of various Microsoft® SharePoint users, from basic users to administrators and developers from organisations of all sizes. The survey was conducted anonymously to find out how SharePoint users perceive SharePoint security and the access rights associated with using SharePoint.

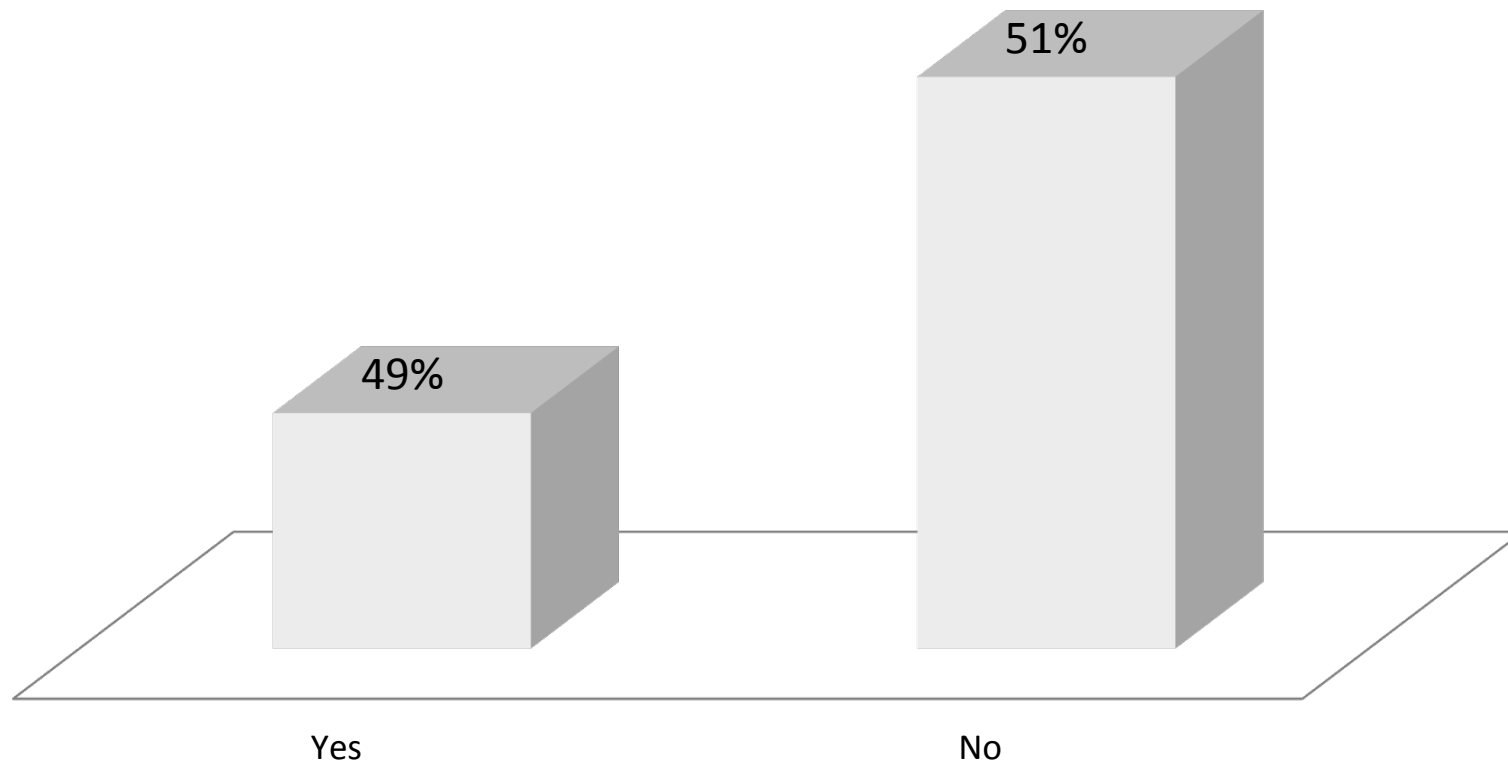
1. What is your SharePoint role in the organisation?



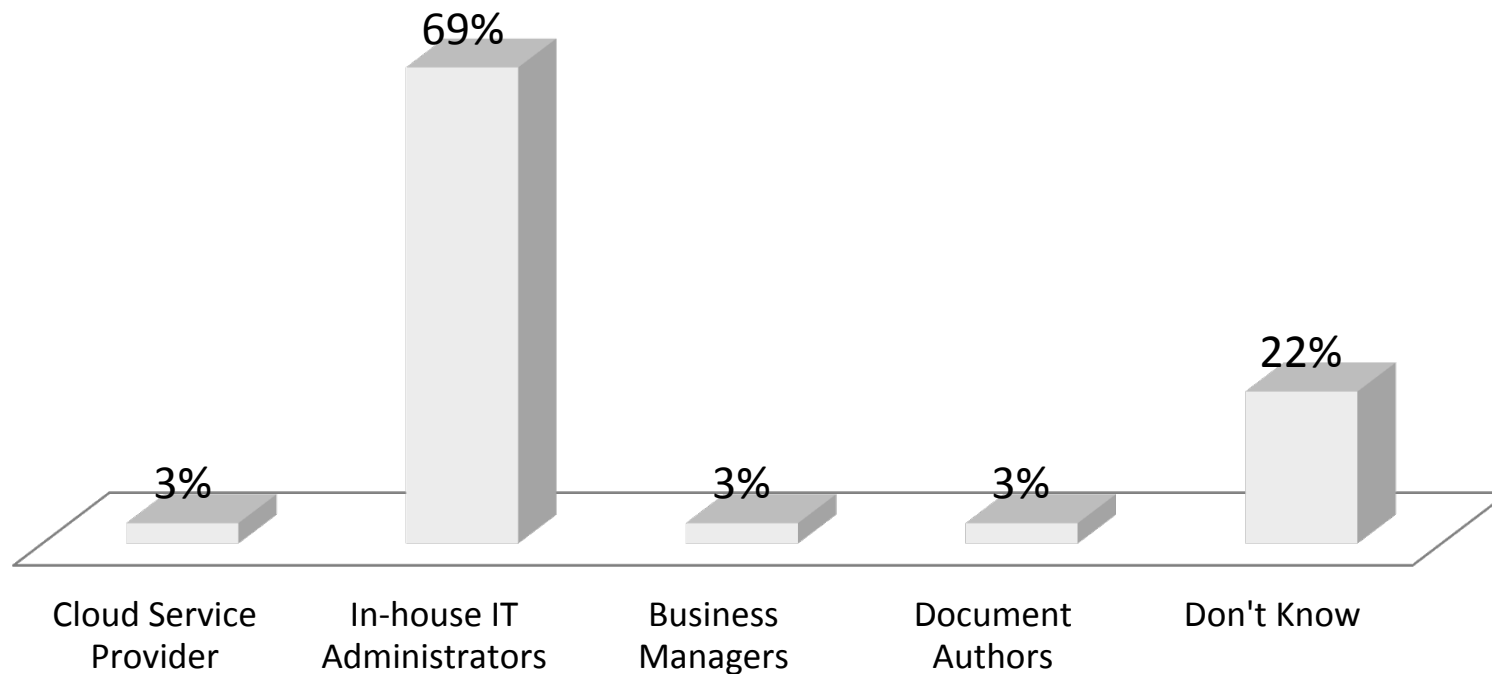
2. What is your organisation size?



3. Are you responsible for managing access rights within SharePoint?

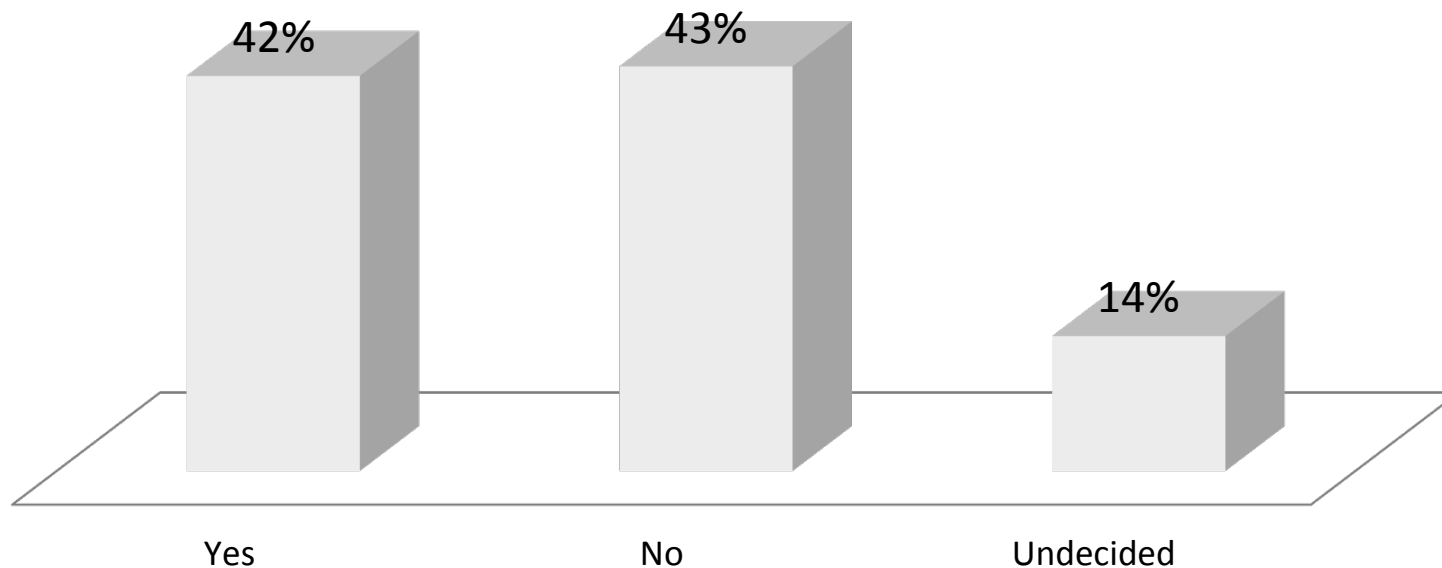


4. If NO: Who is responsible for assigning access rights within SharePoint?



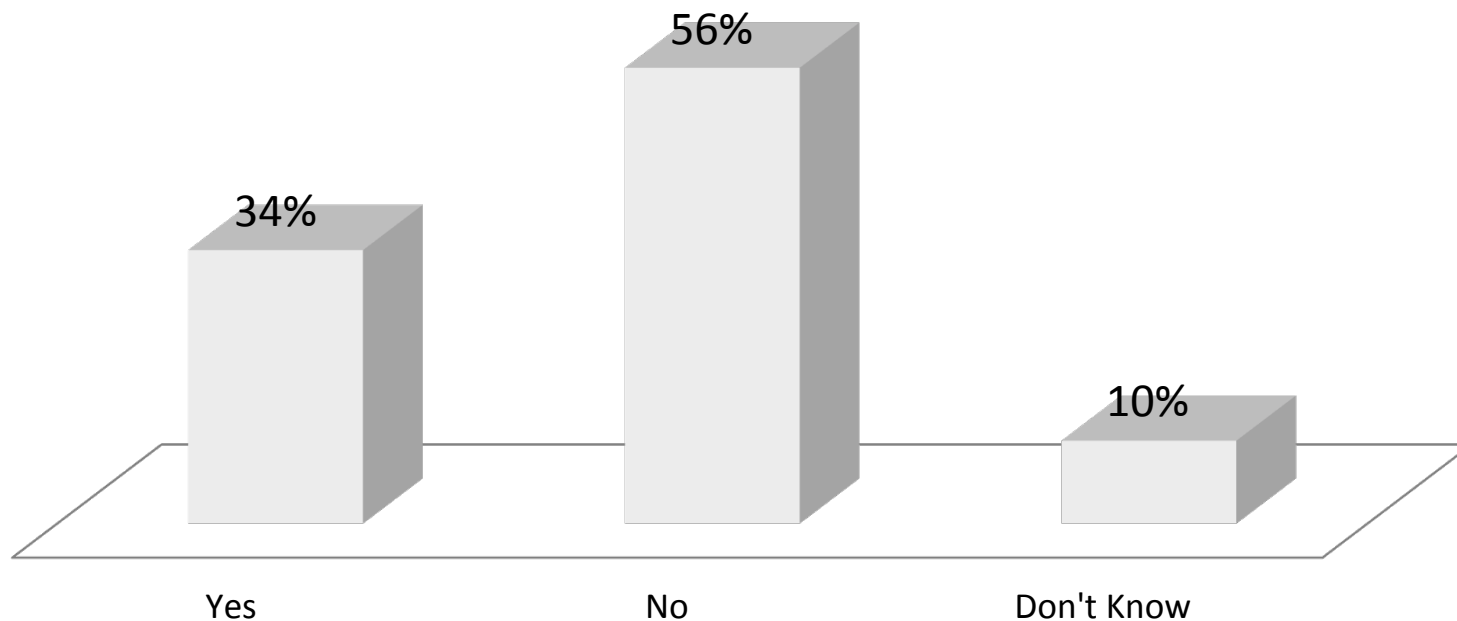
IT Administrators remain overwhelmingly responsible for managing access rights within SharePoint (69%). This share is likely to be even higher, as 22% of users simply didn't know how access rights are managed.

5. Do you think that document authors can be trusted to control who reads the documents they create within SharePoint?



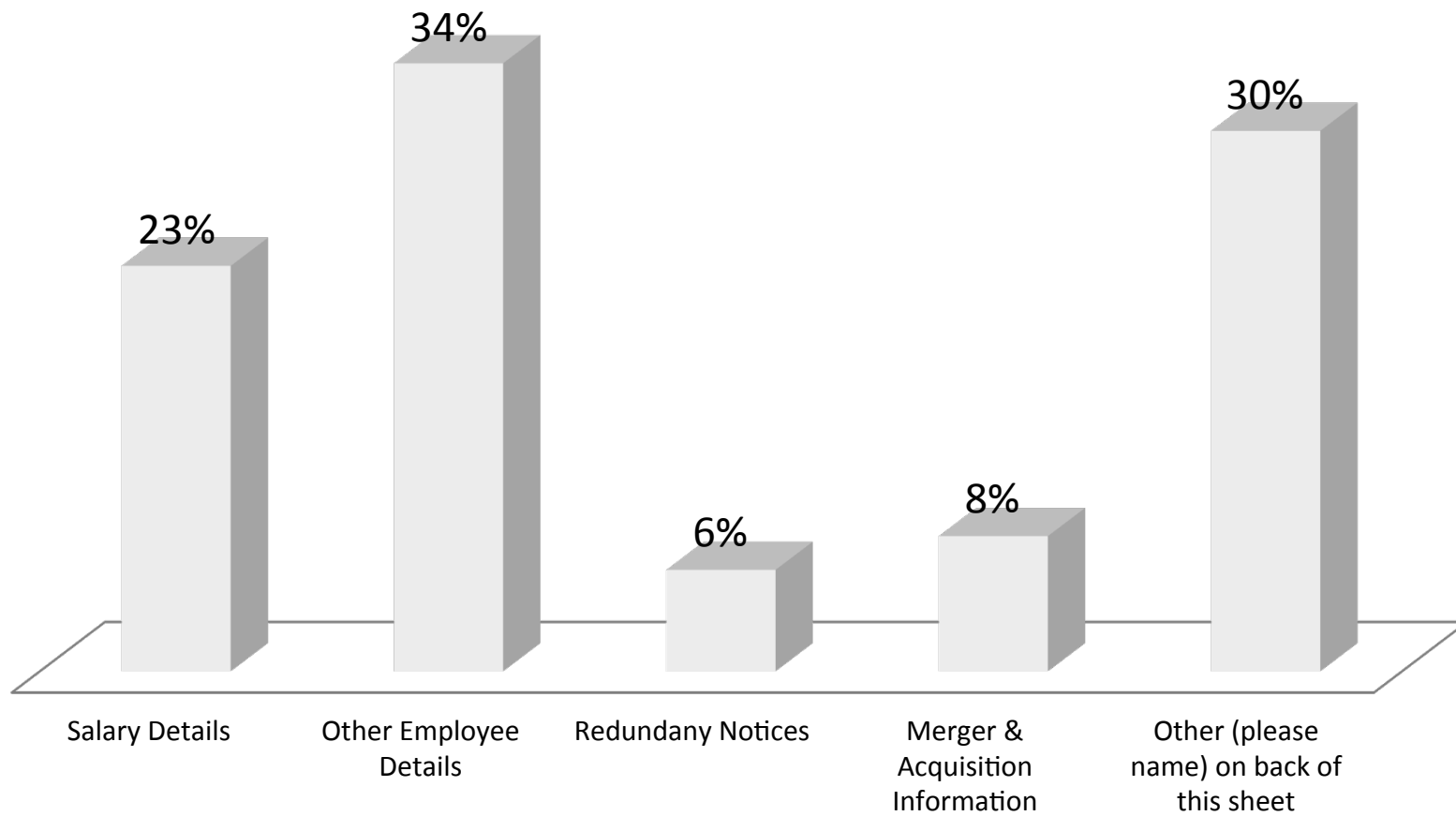
43% do not trust document authors to control who reads the documents they create in SharePoint. IT administrators remain responsible for managing access rights to content even though they are not the people supposed to be using that information. Users are considered competent to send emails to intended recipients, so why is document content management in SharePoint not treated in a similar fashion?

6. Have you or colleagues you know with administration rights ever taken a quick peak at documents that they are not meant to read?

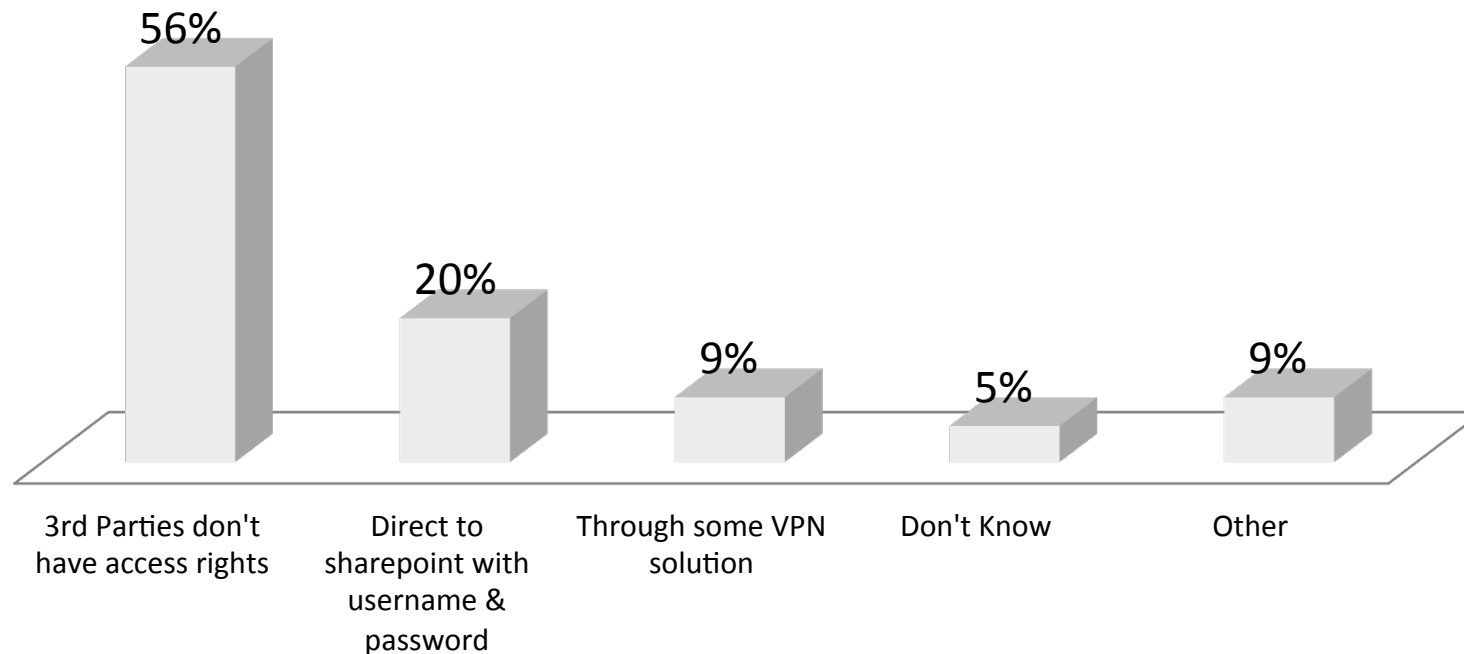


It would appear that a high proportion of IT administrators are more curious than senior management might like to believe. A third of recipients had or knew of others who had looked at documents not intended for them. Administrators have historically held a “God-like” status – oversight of everything, but pure in motive and action. Trusting IT not to look at information they are not supposed to is no longer a tenable position for governance focused organisations with one third of IT administrators potentially looking at other people’s personal details.

6. A) If YES, what sort of documents were accessed?

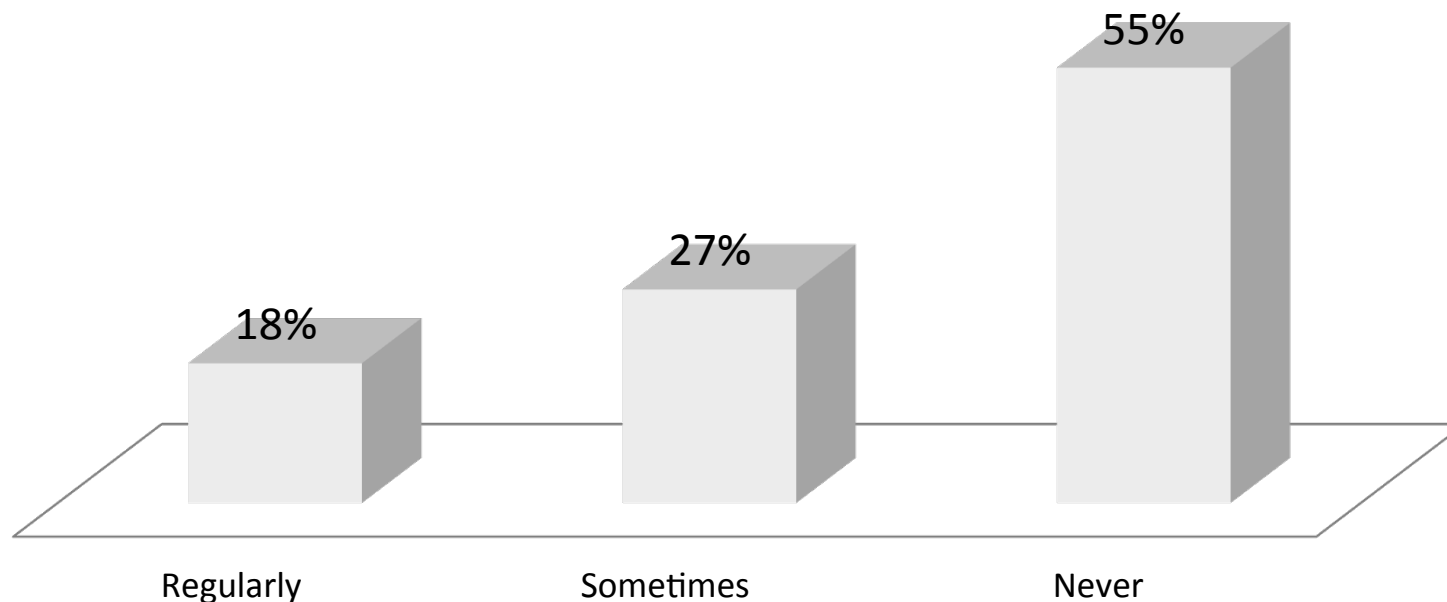


7. How is 3rd party access to your SharePoint environment restricted?



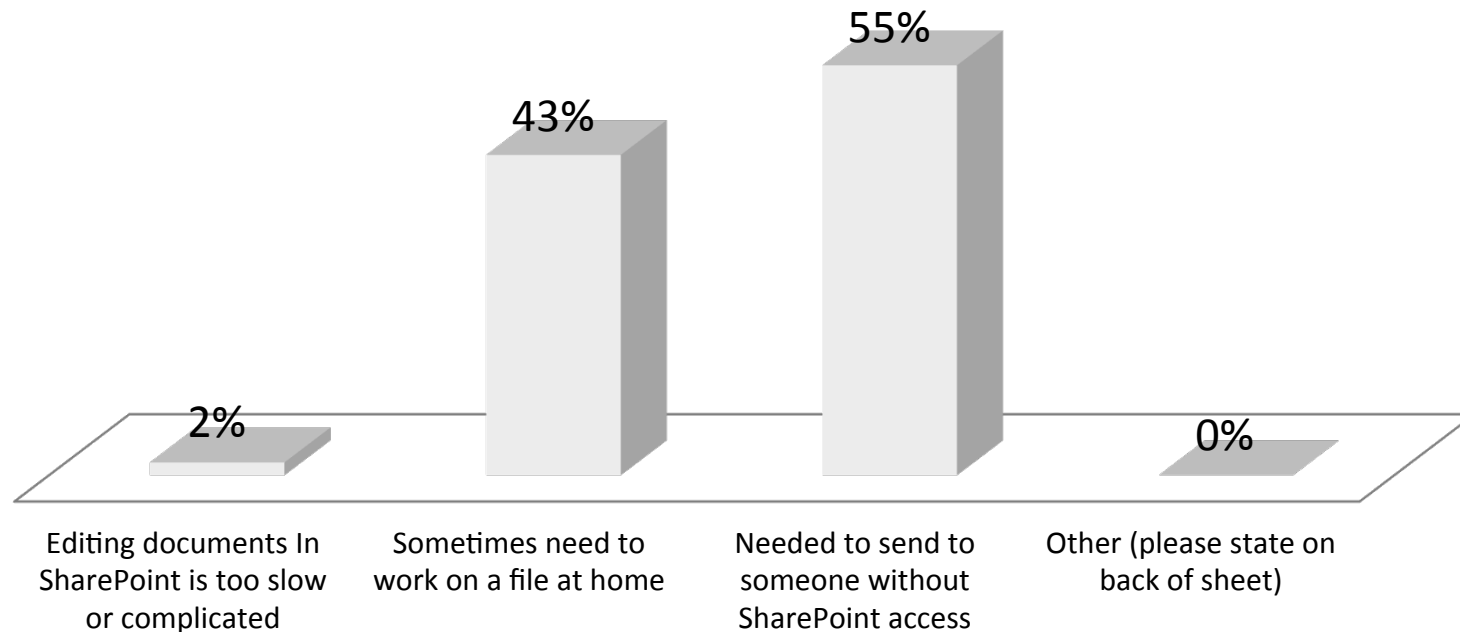
Our findings show that over 50% don't give third party access to SharePoint collaboration environments. It is therefore unsurprising that users sometimes or regularly share information with 3rd parties outside the system.

8. Have you ever copied sensitive or confidential documents from SharePoint to your local PC/USB Key or e-mail to 3rd parties?



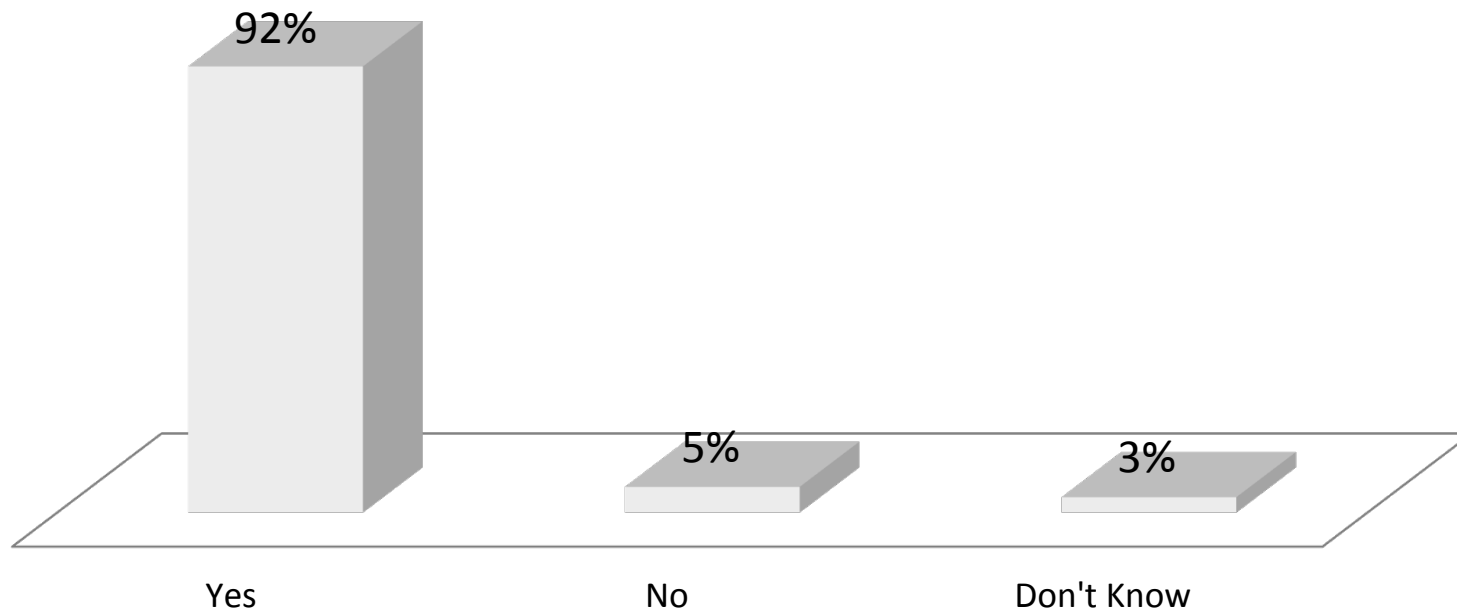
Nearly 45% of users have had an imperative to copy sensitive & confidential information to an unprotected USB stick or an email message which surely circumnavigates the intended purpose of a secure collaboration environment such as SharePoint.

8a) If YES, for what reason did you copy documents out of SharePoint?



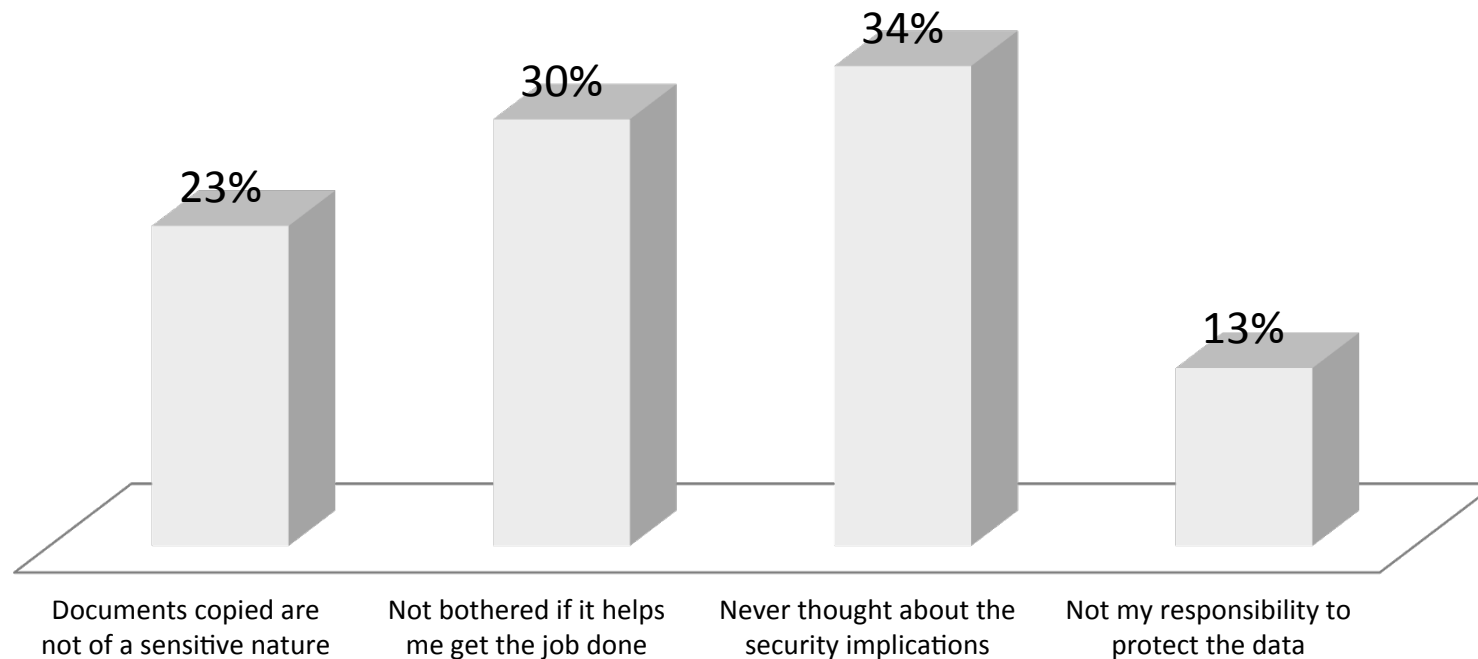
43% of these seemed well intended as they wanted to continue working on documents from home, but surely more reason for IT to provide secure home working to the collaborative environment rather than users resort to such practices which are unlikely to conform to corporate security procedures. Over 55% sent documents to others without SharePoint Access. Whilst the reasons for lack of access were not ascertained it is clear that SharePoint has yet to become an inclusive collaboration tool.

9. Do you realise by taking documents out of SharePoint you are making documents less secure?



The IT security awareness message is being heard but not listened to! Over 90% of those surveyed knew that by taking documents out of the SharePoint environment documents become less secure.

10. If YES, why do you feel the need to take documents out of SharePoint despite the security implications?



A fifth justified this action by indicating documents copied out of SharePoint were not of a sensitive nature; however a staggering 30% said that they were “Not bothered if it helps me get the job done”. A further 35% had never considered the security implications of their actions. Is it any wonder that we see so many data security breaches as a result of irresponsible human behaviour? Organisations need to be coming up with even more innovative methods of communicating cause and effect to their users and perhaps consider sanctions to wake up the 12% that don’t consider it their role to protect corporate information.

Conclusion



The consequences of people circumventing security policies and procedures put in place to protect intellectual property and confidential information within collaboration sites are enormous. We see so many data security breaches as a result of irresponsible human behaviour.

Organisations need to do their own research as a result of our findings, and see how their valuable and sensitive information is accessed by administrators and end users. Organisations need to ensure that they are compliant to laws, regulations and that customer trust is not violated.


Cryptzone recommends that organizations take this research seriously and consider there may be some serious security issues within the organisation that may damage the business seriously. At the end of the day humans can only be as good as the policies, tools and the culture that is provided for them. Organisations need to take steps that allow its workforce to harness the power that SharePoint offers, but still enforce an organisation's policies on data loss. These steps include:

- ❑ Provide better third party access to restricted information held in a SharePoint environment
- ❑ Support encryption of sensitive and confidential documents
- ❑ Ensure that encryption and access management stays with the document regardless of whether the document is moved copied or changed in anyway

About Cryptzone

- The Cryptzone Group is a technology innovator of proactive controls to mitigate IT security risk. We bring together the people, processes and technology to mitigate information security risks identified in the key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security. Headquartered in Sweden, the company has offices in the UK, USA and Poland, as well as an extensive partner network with more than 150 global partners. For more information about the company and its solutions, visit <http://www.cryptzone.com>.
- Cryptzone's share is listed on First North, Sweden, the Nordic alternative market operated by NASDAQ OMX. Certified Adviser is Thenberg & Kinde Fondkommission AB.
- Email: info@cryptzone.com
- Website: <http://www.cryptzone.com>
- For more information please contact your local office:
 - UK: +44 (0) 370 013 1600
 - USA: +1.949.279.6177
 - Sweden & Rest of World: +46 (0)31 773 86 00

About SharePoint Saturday



SharePoint Saturday is an educational, informative and lively day filled with sessions from respected Microsoft SharePoint professionals & MVPs, covering a wide variety of SharePoint-orientated topics. SharePoint Saturday is open to anyone and attracts SharePoint architects, developers, and other professionals that work with Microsoft SharePoint. Events are hosted throughout the year in locations across the world.

For more information visit: <http://www.sharepointsaturday.org>