Kalpa Publications in Computing

Volume 12, 2019, Pages 320–330

Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019


# Office 365 SharePoint Online: Establishing Content Security Awareness with End-Users using Campaigns

Talifhani Sikhitha[1] and Maureen van den Bergh[1]

[1] Applied Information Systems

[1] University of Johannesburg, Bunting Road Campus, Gauteng.

201002496@student.uj.ac.za, maureenvdb@uj.ac.za

**Abstract**

Cloud based information systems such as Office 365 SharePoint Online, could be subject to serious content security risks, because of the lack of awareness of end-users when sharing content in an online environment. Information security awareness campaigns governing the "people problem" of properly securing information systems, are used in aid of organisational efforts towards creating awareness with end-users. Although many research studies determined what should be included in awareness campaigns, they do not always clarify which steps to take to achieve the different elements. The current study contributes its findings to this area of research, by interviewing ten industry experts to determine what practical steps could be taken to achieve the different elements of an awareness campaign aimed at creating awareness among Office 365 Share-Point online end-users. A theoretical model, derived from literature, was presented to experts. Experts were purposively selected because of their knowledge of, and responsibility for, conducting awareness campaigns within their respective organisations. Their recommendations, via interviews, were applied to the theoretical model to include practical steps for achieving the main elements of: addressing user behaviour; including awareness activities and competitions; using multiple communication channels; promoting an information security culture and individual responsibility; having champions for awareness and measuring the effectiveness of awareness campaigns. Future studies could expand this model, both the main elements of awareness campaigns, and the practical steps taken to achieve the main elements.

## 1 Introduction

An organisation that has an online platform offers end-users a great opportunity to be able to interact and communicate in a timely and efficient matter (Al Hasib, 2009). However, this may pose privacy concerns for information that is stored online (Al Hasib, 2009). There are several security risks that are associated with online platforms, and that includes: receiving emails that pose as those that are coming from online platforms, such as SharePoint itself, information leakage when sharing files and links to

external vendors directly from online platforms (Liam, 2013). End-users that are not aware of these security threats fail to protect the organisation's data (Al Hasib, 2009). Organisations that doesn't have user control groups, separation of data, compliance or governance mechanism of data fail to keep track of what the end-users within the company are doing with the data that they are consuming through online platforms (Al Hasib, 2009).

Cloud based information systems such as Office 365 SharePoint Online, could be subject to serious content security risks, because of the lack of awareness of end-users when sharing content in an online environment (Liam, 2013).

Information security awareness campaigns governing the "people problem" of properly securing information systems, are used to aid organisational efforts towards creating awareness with end-users. Although many research studies determined what should be included in awareness campaigns, they do not always clarify which steps to take to achieve the different elements.

In this paper, we address this issue by deriving a theoretical model from literature that includes the main elements of an awareness campaign. The theoretical model is presented to industry experts, for their comments and recommendations on how to achieve each element of an awareness campaign. The paper aims to provide a model that is practical in its application of how to achieve the main elements of an awareness campaign.

# 2 Theoretical Background

## 2.1 Office 365 SharePoint Online

Office 365 SharePoint Online is defined in many ways in various literatures: For example, (Dhouib & Halima, 2013) define it as an online version of SharePoint 2016. (Dhouib & Halima, 2013) discuss that an online version of SharePoint is a cheaper technology that also provides the organisation with more flexibility. While Webber, Mok, & Cheung (2013), define Office 365 SharePoint Online as a technology application that allows business strategies to be aligned with the technology that it provides.

The main goal of an organisation having Office 365 SharePoint Online as their platform, is to maximize the value that is within their information content (Webber, Mok, & Cheung, 2013). Skendzic & Kovacic (2012), describe that an organisation could use Office 365 SharePoint Online for intranet, content storage and knowledge management, which is within Office 365 environment that is hosted in the Cloud. Skendzic & Kovacic (2012), further discuss that an organisation that uses Office 365 SharePoint Online, is mainly interested in features such as sharing content, searching for content, managing content and protecting content using managed permissions. Webber, Mok, & Cheung (2013), point out that the main function of Office 365 SharePoint Online is to allow the organisation to manage the content that was not being managed before, they also mentioned that Office 365 SharePoint Online provides a platform for the organisation's end-users to design and create workflows. Employees can access the system even when they are not within the organisational premises (Rozar, Ibrahim, & Razik, 2013).

Accessing content online enables end-users to be more productive and efficient in their day-to-day activities, whether they are at the organisation's premises or outside the premises. An efficient organisation requires a well-established online system that can be accessible all the time (Dhouib & Halima, 2013). End-users within an organization sometimes prefer to work even after business hours, which means they should be able to access content anywhere and at any time to be able to work. Content security is a concern when it comes to the organisation's access to information, and whether end-users are aware that the content that they are accessing always has to be treated as sensitive (Caldwell, 2016). End-users share links with external vendors without realizing that it affects reporting processes. This is

due to end-users not being aware of the changes that happen in the background. An organisation could avoid this security risk by creating awareness campaigns (Ahlan, Lubis, & Lubis, 2015).

Johnson (2006), indicates that awareness can help to improve the behavior of users towards content, and that lack of content awareness is becoming an increasing problem in organisations. Ahlan, Lubis, & Lubis (2015), established that content breach incidents are still occurring in organisations despite the policies and procedures that organisations are enforcing on end-users. Strother (2002), mention that an organisation should constantly deliver effective training to its end-users (Liam, 2013). However, Johnson (2006), showed that it can be difficult to influence end-users on how to conduct themselves toward the use of information, because they are not trained or are un-aware that their behavior many affect the security of content.

Office 365 SharePoint Online could be subject to serious content security risks (Liam, 2013). Liam (2013), established that Office 365 SharePoint Online security risks include: lack of SharePoint content awareness, inadequate or non-existent audit trails for SharePoint Usage, inadequate administrative access of SharePoint content awareness, failure to secure SharePoint against privileged insider accounts, and misconfigured access controls and permissions. Of these, one of the most common security risks, is the lack of SharePoint content awareness by end users (Liam, 2013).

## 2.2 Office 365 SharePoint Online

Content awareness together with communication cover a wide range of topics that are required to fulfil the organisation's requirements (Ki-Aries & Faily, 2017). Traditionally, when an organisation implements an awareness program, they would also have awareness campaigns (Ahlan, Lubis, & Lubis, 2015).

The term "campaign" is used to refer to awareness strategies within an organisation and campaigns are created as activities to achieve the organisation's desired goals and communication (Marshall, 2008). Kajzer, D'Arcy, Crowell, Striegel, & Van Bruggen (2014), state that awareness programs are created to communicate the risks associated with the organisation's information, while campaigns raise an individual's responsibility towards the organisation's resources (Kajzer, D'Arcy, Crowell, Striegel, & Van Bruggen, 2014) . However, with awareness campaigns, it is difficult to know whether the communication that is conveyed will be effective (Kajzer, D'Arcy, Crowell, Striegel, & Van Bruggen, 2014) .

Bharakda (2015), mentioned that if an organisation wants to address underlying issues and conduct successful awareness campaigns, they can achieve it by using the following steps: the organisation should establish the objectives of the campaign, establish the target audience that they want to send the communication to, establish the main purpose of the campaign (research why the campaign is needed), and ensure that the awareness campaign is measurable.

End-users that are trained about the importance of awareness, are more likely to have a positive attitude towards the security of content (Ahlan, Lubis, & Lubis, 2015). But with online programs such as Office 365 SharePoint Online, traditional awareness methods may or may not be appropriate (Rozar, Ibrahim, & Razik, 2013). O'Connor (2014), stated that key objectives when conducting awareness campaigns for Share- Point includes end-users adapting to the system quickly and improving productivity.

End-users should have a certain level of understanding to ensure that they know the organisation's systems and that data within said systems is secured (Caldwell, 2016). Fischer-Hübner, et al. (2013), mentioned that there should be infrastructures in place to manage and identify awareness techniques for end-users. Furthermore, for programs to be successfully implemented, the current online platforms should be improved in order to increase awareness across end-users (Fischer-Hübner, et al., 2013). O'Connor (2014), established that awareness campaigns in SharePoint should include the following communication channels: embedded targeted e-mail, business unit presentations, town halls, dedicated SP communication site, newsletters, brown bags or lunch and learns, and webcasts (see Figure 1):

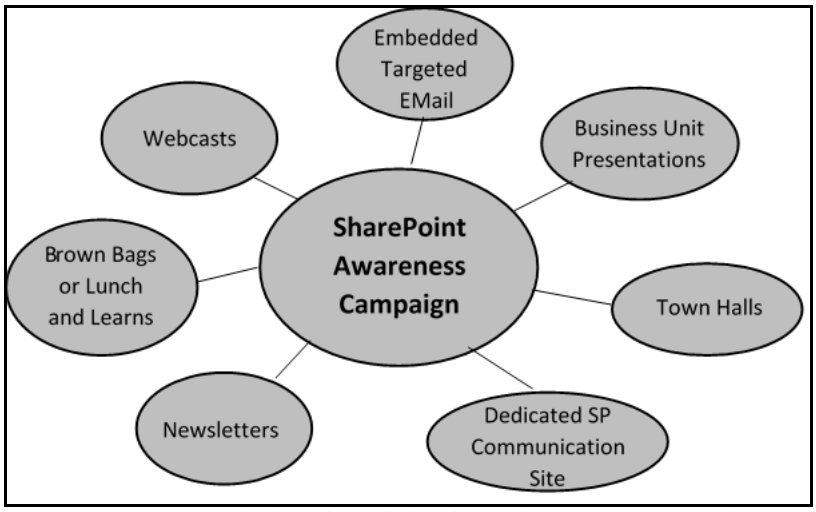


**Figure 1:** Communication Channels for SharePoint Awareness Campaigns

Further, Caldwell (2016), established that an organisation should have an effective awareness culture, while taking the following processes into account: select the correct audiences, by using the term "employee", rather than the term "user", using the right tone to address the audiences is essential to ensure that each and every user understand their role, and always keep the employees informed.

Moreover, implementing user awareness campaigns, by educating and training end-users can help to improve the use of systems (Ghazvini & Shukur, 2016). However, as mentioned by Caldwell (2016), awareness without any other activity is not enough. An organisation should also conduct competitions for end users. This will ensure that end-users take awareness seriously (Caldwell, 2016). Furthermore, an organisation could create a reward program for those users that are using the system effectively (Ahlan, Lubis, & Lubis, 2015), and additionally organisations should nominate system leaders that will be champions for awareness campaigns and that will also support end-users (Johnson, 2006).

Furthermore, a model that was generated for awareness campaign includes having multiple communication channels for end-users and providing end-users with rewards programs and competitions. This will ensure that end-users take awareness seriously (Caldwell, 2016).

# 3 Theoretical Model for Information Security Awareness Campaigns

A review of literature identified the following 8 main elements that should be included in an awareness campaign, namely: addressing user behaviour; including awareness activities and competitions; using multiple communication channels; promoting an information security culture and individual responsibility; having champions for awareness and measuring the effectiveness of awareness campaigns.

Figure 2 shows the theoretical model that was constructed from a review of the literature, for the purpose of this study.

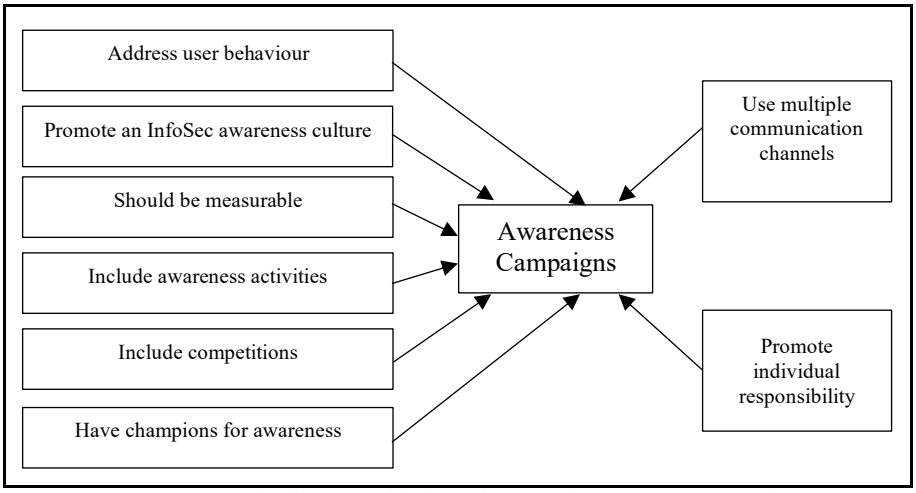


**Figure 2:** Main elements of information security awareness campaigns

# 4 Research Methodology

The data collected and used in this qualitative study were from a sample of purposively selected industry experts, with knowledge of, and responsibility for, conducting awareness campaigns within their respective organisations. Industry experts reside within South African organisations that are actively promoting awareness campaigns, aimed at establishing content security awareness with Office 365 SharePoint Online end-users.

Industry experts were contacted via email and invited to participate in this study. Upon acceptance, data collection took place via face-to-face semi-structured interviews with ten participants. At the start of each interview, the purpose of the research was reaffirmed again to each participant's voluntary consent, and that interviews will be voice recorded. Participants were also told that their data will be confidential and that it would only be used for academic purposes. After giving their consent, a theoretical model derived from literature was presented to the participants. Once participants studied the model and any confusion was clarified, the participants were asked to comment on each individual element within the model and recommend practical steps they are using for achieving each one.

# 5 Results

Results are discussed in this section and supported via verbatim quotes from participants. The 8 main elements of an awareness campaign include: addressing user behaviour; including awareness activities and competitions; using multiple communication channels; promoting an information security culture and individual responsibility; having champions for awareness, and measuring the effectiveness of awareness campaigns.

## 5.1 Address User Behaviour

For some participants, addressing user behaviour means working directly with the users. To address user behaviour, one participant stated that they use positive reinforcement during awareness campaigns, by recounting examples of other users within their own organisation, and their successful use of Office 365 SharePoint Online. "User behaviours differ, some users are prone to using Office 365 SharePoint

Online, because they know about it and have worked with it. Some are skeptical because they don't know anything about the platform, or they have misconception about what the platform can do. So, we use success stories of what the platform can do." Another state that following on their awareness campaigns, behaviour training will take place. "The organisation has behaviour training, in a sense that they would ask questions related to your behaviour towards content and they would raise a flag of how secure your behavior is, then give you tip and tools on how to change that behaviour." While another mentions the importance of end-users' knowledge about various campaigns. For example, protecting their SharePoint passwords that in itself create awareness amongst their users. "I think it's good that users are aware of different campaigns and know about different ways people can protect password. This is related to SharePoint." A more indirect approach is followed by others that will send their users targeted communications when they notice irregular online behaviour, from their monitoring of Office 365 SharePoint Online reports. "The only way we can know is by looking at a report that we get online, like internal sharing and external sharing of information in SharePoint, those are the reports or dashboards that we can use to monitor user behaviour and trend. Based on that information we can determine the plan to increase awareness. For example, if we see a sudden spike in internal sharing, we can use that information to send communication based around it."

## 5.2 Promote an InfoSec (Information Security) Awareness Culture

To promote an Office 365 SharePoint Online content security awareness culture, participants send end-users communications that explain how things are done in the organisation with regards to content security, "using the same mechanism mentioned previously like email." While another state a preference for digital channels, because they find emails difficult to monitor. "Using digital channels like SharePoint and Yammer…we prefer something that is web based because emails are difficult to monitor." A different approach mentioned by a participant, is that they promote an innovation culture, where their end-users are rewarded for providing suggestions for improvement of document management via the Office 356 SharePoint Online platform. "We have an innovation culture, were people get rewarded for innovation. Those initiatives are supported for end-users to get to use the platform and get to know how they can manage documents"

## 5.3 Should be Measurable

For almost all participants, included in their responsibilities are measuring the success of awareness campaigns. They do this mostly by sending end-users surveys to complete, "We have surveys that we send out our end-users…we prefer to use surveys." Surveys are used to "measure that the key lessons or key objectives are met…it is transparent and simple to measure the number of people and what feedback they are giving us." However, one mentioned that this responsibility falls outside their portfolio, and the organisation's information security team assesses results from assessments completed by end-users, "There is no real measurement form our side, I believe the information security team has a record of who is doing what and send out reminders for exams and look at the assessment that you do."

## 5.4 Include Awareness Activities

During awareness campaigns, to actively involve users, awareness activities such as online scenario-based questionnaires, online interactive surveys, and online treasure hunts are used. These online activities are all utilizing features from within Office 365 SharePoint Online itself. As mentioned by a

participant, “you can use SharePoint itself and send out questionnaires so that users can familiarize themselves with scenarios of how you can protect content” and another stated “we use interactive surveys.” Using treasure hunts, a participant declared that “we do treasure hunts, we hide content within SharePoint for users to go and find them, then through that, they get to be aware of content and then they get rewarded for participating.”

## 5.5 Include Competitions

A diverse set of prizes are recommended by participants. Users could win vouchers with a monetary value, “here's a lot of incentives and prizes and monetary value, so there's a couple of things that people can win” or users could win tickets, “people always respond to winning something or tickets to an event” or winning branded organisational items “prizes are more effective or branded items. Things that are not readily available from outside shops.”

## 5.6 Have Champions for Awareness

Champions for awareness are mostly selected by participants and trained to actively contribute to awareness campaigns. During awareness campaigns they will participate and afterwards they continue to advocate content security awareness within their respective environments, both online and physical environments. Champions for awareness are usually content owners, active users that are excited about the product, site administrators, or nominated champions. Participants find that content owners are a good choice to have as champions for awareness, “What we do, we usually have someone who owns the content, not really capture the content, but someone who is responsible for the ownership of that content. So we would likely choose that person as a champion and also someone who has been trained.” Also active users that are ardent about the product, who are able to influence others positively towards the product, “We look at how people are excited for the platform and people who are active users. People who can have a good influence to their colleagues, to tell them that I’ve used this platform and this is how it helped me. That way they are excited about the product.” Site administrators also proof to be good champions of awareness. Participants see who the administrators for the sites are, and those will be the people trained to manage the site, “When the site is designed, you build it around who needs access and site owners are basically the gate keepers to ensure that the security is set out and is enforced going forward and there is approval from them before we assign any permission.” Sometimes champions are nominated by others within the organisation, “We don't actually select it; the business will put forward a champion. There are people who are very keen, and when we find them we train them to become champions.”

## 5.7 Use Multiple Communication Channels

All participants mentioned mostly using emails to communicate to users, information about awareness campaigns, and to communicate with users during awareness campaigns. They use both ordinary company email platforms and targeted email via Office 365 SharePoint Online. As one mentioned “we mainly use email“ and “like I mentioned, it's not only online services such as Yammer (an social networking service used for private communication within organisations (Collins English dictionary, 2018)), but email as well, everyone checks emails.” With another stating that “the communication channels we use is SharePoint which triggers email that is sent to users that are targeted.”

Banners during awareness campaigns are also used to communicate the “message of the day.” As one participant found out that “putting up banners can create awareness because visually you can see it

while walking around," while another uses looped videos during awareness campaigns. Usually participants use a combination of the mentioned communication channels.

## 5.8 Promote Individual Responsibility

Encouraging end-users to take individual responsibility for the security of information in their organisation, participants mention fostering accountability with their users, actively affirming the consequences of non-compliance, promoting knowledge sharing (portal), and performing ad hoc reviews. Accountability is managed by setting permissions for end-users and holding them answerable when there are security issues within their content area. "How we set up the permission and then we know that it's maybe 5 people responsible for that content and we know who to hold accountable for if there are any security issues." By actively affirming the consequences of non-compliance,

"It comes down to proper administration and reports, on knowing who is using what and what they are doing, and telling them that if they don't follow security there will be consequences**.**" Involving end-users in the process of knowledge sharing and creating a sense of inclusion, are seen by some as promoting responsibility. "More engagement…a SharePoint portal where they can log questions and have a FAQ around specific things." Others find ad hoc reviews encourage individual responsibility when end-users know a review could take place at any time. "We review the manager or super user of specific department or piece of content, then review the users that have access to that content."

# 6 Discussion

The aim of this study was to determine the practical steps that could be taken to achieve the different elements of an awareness campaign aimed at creating awareness among Office 365 SharePoint online end-users. From the insights gleaned from participants, the model in Figure 3 is presented as a possible solution.

All participants agreed that it is good practice to address user behaviour via awareness campaigns. Whether behaviour is addressed directly with the user or indirectly via targeted communications. Using positive reinforcement during awareness campaigns, by recounting the success stories of other Office 365 SharePoint Online end-users, creating awareness of awareness campaigns, conducting training after awareness campaigns, or using targeted communications, are all aimed at addressing user behaviour.

But to get end-users actively involved during awareness campaigns, awareness activities are most effective. Utilizing Office 365 SharePoint Online features, such as online scenario-based questionnaires, online interactive surveys, and online treasure hunts to draw end-user "into" the awareness campaign. Sometimes even combining active involvement with a reward, such as prizes that include monetary vouchers, tickets to an event, or branded organisational items that can't be bought somewhere else.

As their preferred communication channel, most participants will use email to communicate information about awareness campaigns to users, and to communicate with users during awareness campaigns. Using both ordinary company email platforms and /or targeted email via Office 365 SharePoint Online. Although banners and looped videos are used during awareness campaigns because of their visual impact to convey the "message of the day," participants find email communications more effective as a communication tool. However, when a more personal touch is required, appointing, training and using champions of awareness is the route to follow. Wanting to influence other end-users positively towards the product, participants involve champions for awareness, such as content owners, active users that are excited about the product, site administrators, or nominated champions. Champions for awareness participate in awareness campaigns, but importantly continue creating awareness even after campaigns have ended. They will continue to advocate content security awareness within their respective environments.

This links to creating an information security awareness culture within their respective organisations. Participants differ in their application of practical steps of how to explain to end-users, how things are done in the organisation with regards to content security. Some prefer email, others rather use digital channels, stating that emails are difficult to monitor. An interesting approach mentioned by one participant is that they promote an innovation culture. In this culture their end-users are rewarded for submitting ideas to improve document management via the Office 356 SharePoint Online platform.

To encourage users to take responsibility for what they do online and the security of information in their organisation, participants mention here their own preferred processes. Some prefer fostering accountability with end-users, while other prefer upholding the consequences when end-users do not comply, yet another prefer including end-users in the process of knowledge sharing, and still some find that ad hoc reviews encourage individual responsibility, especially when end-users know a review could take place at any time.

All participants mention that the effectiveness of awareness campaigns should be measured. In determining a return on investment, they mostly use surveys. Surveys are easy to use and provide insight about the extent to which awareness campaign key objectives were met.

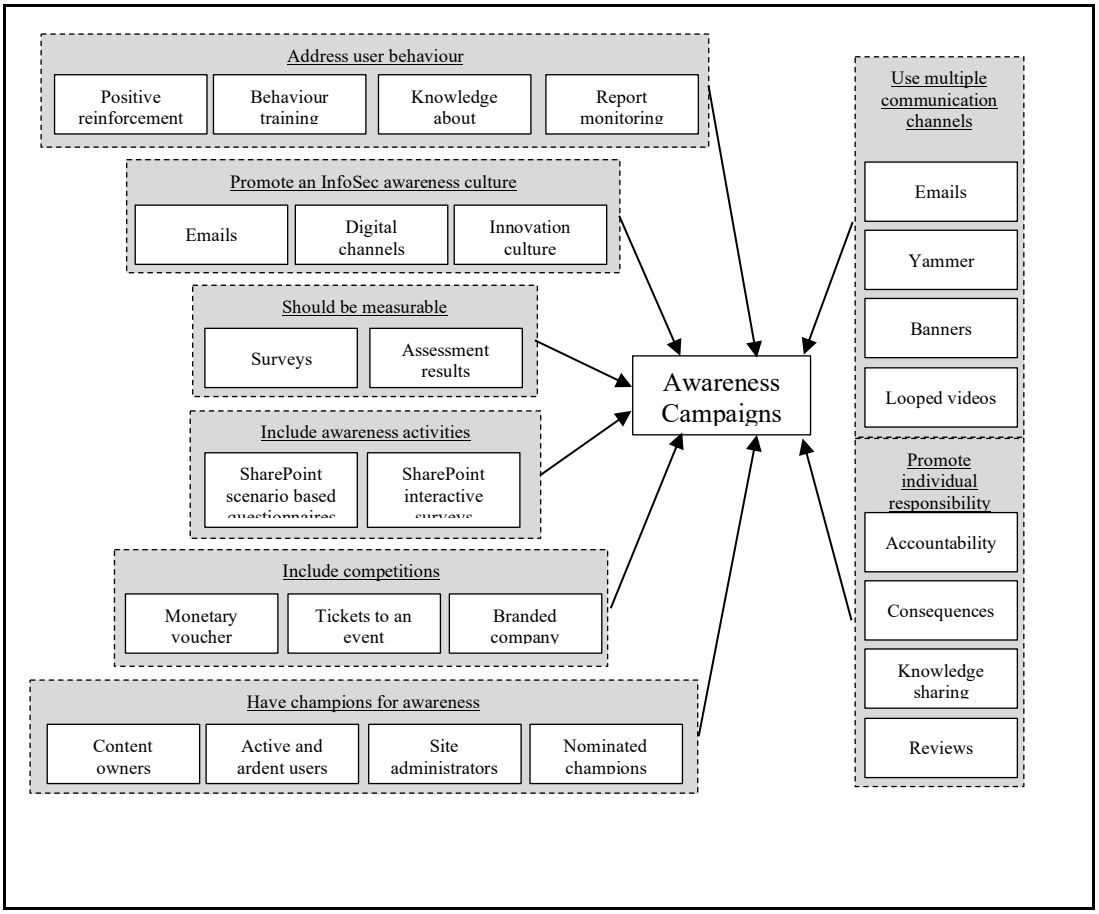


**Figure 3:** Model proposing practical steps to achieve the main elements of an awareness campaign

# 7 Conclusion

Creating awareness amongst end-users for cloud-based information systems such as Office 365 SharePoint Online, is important because the system could be subject to serious content security risks. Information security awareness campaigns is one method of achieving awareness. However, the practical steps taken to achieve the main elements

of awareness campaigns aren't always clarified. The current study presented practical steps, recommended by industry experts, to be taken to achieve the different elements of awareness campaigns.

In recommending practical steps for achieving the main components of an awareness campaign, participants varied experiences produced a diverse set of steps to choose from. Although a good foundation to build on, this is by no means an exhaustive list of steps. The practical steps recommended by industry experts should be received as just that, "recommendations." Organisations should decide which of the practical steps would be most appropriate for their end-users and their specific environment.

Further research could expand the model to include additional main elements of awareness campaigns, as well as additional practical steps for achieving the main elements.

# References

Ahlan, A. L., Lubis, A., & Lubis, M. (2015). *Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures. Procedia Computer Science,72, pp.361-373.*

Al Hasib, A. (2009). *Threats of online social networks. IJCSNS International Journal of Computer Science and Network Security, 9(11), pp.288-93.*

Bharakda, A. (2015). *5 steps implementing a successful awareness campaign*. Retrieved 04 11, 2019, from http://www.documentcapture.co.uk/2015/01/5-steps-implementing-successful-awareness-campaign/

BSI Group, S. A. (n.d.). *End User Security Awareness Training*. Retrieved 04 11, 2019, from BSI Group South Africa: https://www.bsigroup.com/en-ZA/Our-services/Cybersecurity-Information-Resilience/Technology-solutions/End-User-Security-Awareness-Training/

Caldwell, T. (2016). Making security awareness training work. . *Computer Fraud & Security 2016(6)*, pp.8-14.

Dhouib, S., & Halima, R. (2013). Surveying Collaborative and Content Management In Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). *2013 IEEE 22nd International Workshop* (pp. pp. 299-304). IEEE.

Fischer-Hübner, S., Hoofnagle, C., Krontiris, I., Rannenberg, K., Waidner, M., & Bowden, C. (2013). *Online Privacy–Towards Informational Self-Determination on the Internet.* Digital Enlightenment Yearbook.

Ghazvini, A., & Shukur, Z. (2016). Awareness Training Transfer and Information Security Content Development for Healthcare Industry. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS 7(5)*, pp.361-370.

Johnson, E. (2006). Security awareness: switch to a better programmeme. *Network security 2006(2)*, pp.15-18.

Kajzer, M., D'Arcy, J., Crowell, C., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & security, 43*, pp.64-76.

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *computers & security, 70*, pp.663-674.

Liam. (2013). *Top 10 SharePoint Content Security Risks and What to Do About Them*. Retrieved 04 11, 2019, from ITProtoday: http://www.itprotoday.com/security/top-10-sharepoint-content-security-risks-and-what-do-about-them

Marshall, T. (2008). Campaign. In Design Dictionary. *Birkhäuser Basel*, pp. 62-63.

O'Connor, E. (2014). SharePoint 2013 Field Guide: Advice from the Consulting Trenches. *Sams Publishing*.

Rozar, N., Ibrahim, A., & Razik, M. (2013). Comparing effectiveness of e-learningtraining and traditional training in industrial safety and health. In Transdisciplinary Marketing Concepts and Emergent Methods for Virtual Environments. *IGI Global*, pp. 214-229.

Skendzic, A., & Kovacic, B. (2012). Microsoft office 365-cloud in business environment. In MIPRO, 2012 Proceedings of the 35th International Convention. *IEEE*, pp. 1434-1439.

Strother, J. (2002). An assessment of the effectiveness of e-learning in corporate training programmes. *The International Review of Research in Open and Distributed Learning, 3(1)*.

Webber, T., Mok, W., & Cheung, K. (2013). Proposed use of sharepoint to improve new employee in-processing. In e-Business (ICE-B), 2013 International Conference. *IEEE*, pp. 1-8.