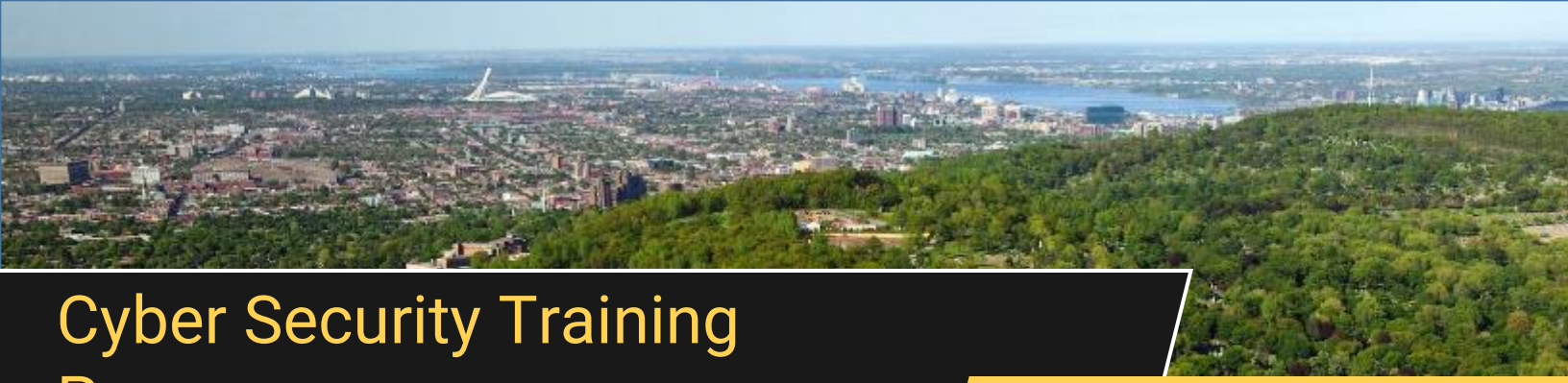

Cyber Security Training Programs

Adeline Veyrinas, Master's candidate

RCCP Research Chair in Cybercrime Prevention

Briefing Note
Vol. 1 Iss. 3

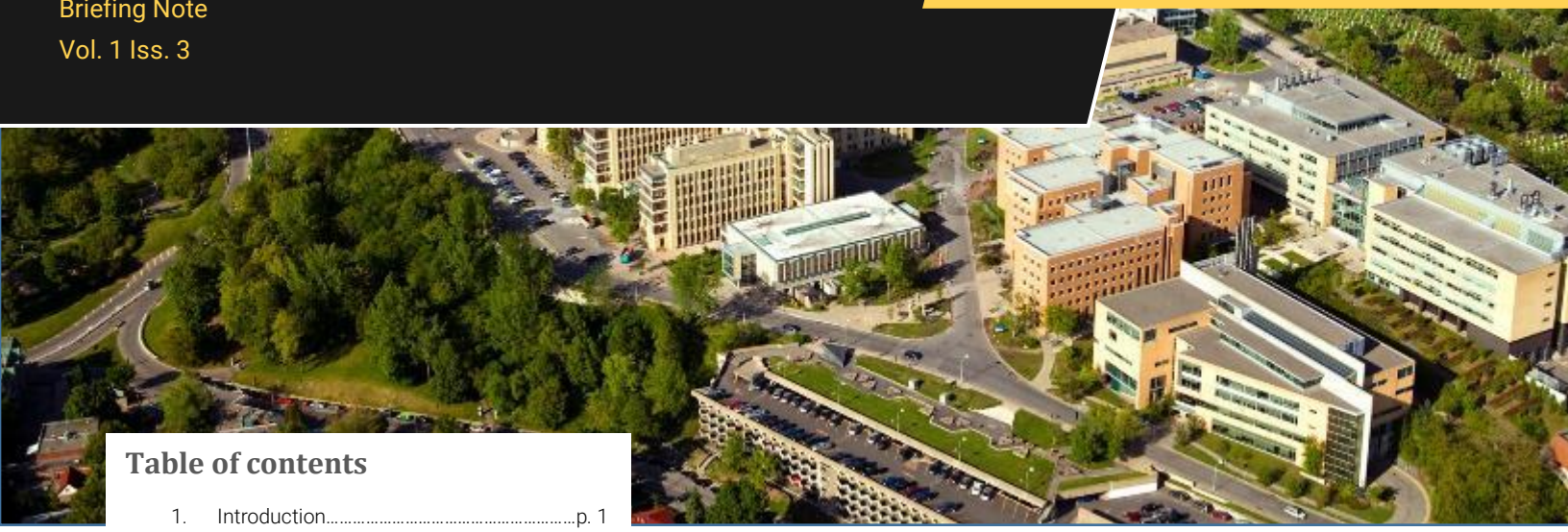

Table of contents

The Research Chair in Cybercrime Prevention was created on the initiative of the University of Montreal, Desjardins and the National Bank of Canada. Led by Benoît Dupont, researcher at the International Centre for Comparative Criminology at the University of Montreal, its mission is to contribute to the advancement of research on cybercrime phenomena from the perspective of its prevention.

Introduction

According to Statistics Canada,[1] **21% of Canadian businesses reported that they had a cyber security incident in 2017. Of those incidents, 23% involved the theft or attempted theft of personal or financial data.**[2] This kind of cybercrime can cost companies dearly in terms of money and reputation.[3] For example, money services businesses reported that their employees fell behind on their day-to-day activities (71%), fewer employees were available for day-to-day work while they dealt with the incident instead (75%), and they saw a drop in revenue (51%).

Canadian companies now need to figure out how the "human factor" can help them prevent cyber threats. In 2018, 34% of data breaches were instigated internally, and 33% of those breaches were social engineering attacks targeting employees.[4][5][6]

That's why it's important to address what companies still need to do to prevent data breaches, and ask questions like: what are their priorities when it comes to the "human factor"—the catalyst behind certain cyber attacks? In this briefing note, we review where companies currently stand, lay out the main solutions proposed in the literature and suggest what improvements could still be made. Lastly, we go over how companies can apply this information in a practical way.

How companies can prevent data breaches

Even though companies use IT solutions to secure their systems, it seems that the leading cause of confidential data breaches is human or employee behaviour.[7] In 2019, phishing was the leading cause of data breaches in US companies.[6 8 9]

Yet preventing these kinds of incidents is no small feat; even when employees know the company policies, they rarely follow them, if at all.[10 11 12 13]

The two main methods being used to help employees change their behaviour and manage information more securely are **awareness** and **training**.[14] Awareness tunes people into the risks of cyber attacks and increases their sense of accountability, but on its own, it's not enough to convince them to adopt safer behaviour.[7] Training, on the other hand, teaches them the skills they need to detect and deter incoming threats.[55] In fact, training is often considered the best preventive measure against information security threats because it involves people directly.[15 16]

Information security training can be individual or group-based;[17] the two approaches focus on distinct but complementary aspects of awareness and safe information security behaviour.

Information security training methods

The collective approach: Collaboration groups

One way to train participants to become more aware and change risky behaviour is through **collaboration groups**. These consist of small, short workshops delivered to a select group of people (like employees in the same role or level in a company). An instructor, expert in a specific area, generally facilitates the workshops. They encourage participants to dialogue with their colleagues through group discussions on a given topic.[18 19 21]

Among the different methods used to increase participant awareness and train people on information security, collaboration groups are considered one of the most effective. That's because they draw inspiration from behavioural adaptation theories,[20] touching on topics such as **subjective norms** and **active participation**.

Getting people involved and motivated: Active participation

Collaboration groups encourage **participants to get involved** through group discussion workshops.

Getting people involved is an important part of getting them to adopt certain behaviours according to several theories, including the **buy-in theory of participation** and **participation theory**. According to these theories, the more involved someone gets in a given task and the higher their potential impact on it, the more important and relevant it becomes to them. They'd thus be more inclined to adopt the corresponding attitudes and behaviours and participate in related activities.[3 21]

Because collaboration groups encourage participation (through sharing knowledge, collaborating, having group discussions, getting involved), participants can:

- **Adopt efficient solutions** through group discussion exercises rooted in Mindspace techniques.[22 23 24]
- **Increase their understanding and sense of accountability** in terms of risk prevention by individually reflecting on the issues and seeking solutions.[30]
- **Change their attitude** and behaviour toward information security thanks to how invested they have been in the training.[7 33]

Adopting a positive attitude: Interpersonal trust

Through dialogue and group discussions, collaboration groups can encourage employees to adopt a positive attitude toward safe behaviour. But wanting to respect **social norms**[25] also plays a significant role. Several behavioural change theories back this up, including:

- The **social bond theory**, which explains an individual's behaviour through their relationships with their peers: The more they take part in the activities and behaviours they defined together, the less they're likely to break from them.[3]

- The **theory of planned behaviour**, which draws on the notion of subjective/personal norms[26] to explain why individuals choose to adopt certain behaviours.[27 28 29]

- The **elaboration likelihood model**, which addresses how persuasive arguments can influence individuals to integrate and accept certain information.[13]

Exchanging with colleagues, assessing what others expect of you and transferring knowledge by interacting with others all encourage **social bond** and trust, which is one of the foundations for adopting a specific behaviour.[30]

In fact, **social bond**:

- Lets people gain a **better understanding** of a given topic through active dialogue with peers who have a similar level of knowledge.[30 31]

- Helps them **build awareness and knowledge** through knowledge transfer via dialogue with colleagues and the instructor.[30 32]

- **Motivates them to change their behaviour** by virtue of having participated in the collective process of promoting safe information security behaviour.[30]

In sum, through the concept of **positive interdependence**,[32] collaboration groups encourage **collaborative learning**, whereby individuals working together on a task lean on each other to understand, integrate (gain a sense of accountability) and motivate one another to achieve a given goal.[33 34 40]

However, this approach has some limits that we should keep in mind if we want to implement it:

- It's **costly** in terms of time,[18 19] money and manpower. It also requires lots of preparation, considering that we first have to identify the priority needs of each company in terms of cybercrime prevention. This part is crucial to determining the key points the training would need to address.

- It needs to be implemented long-term and continually over time if participants are to integrate the lessons and change their attitude and/or behaviour.

- Its effectiveness is difficult to determine because of its qualitative features, which require adapted tools for measuring results over time.[19 35]

The individual approach: Computer-based training

The second learning method is **computer-based training (CBT)**, through which users take part in an interactive learning process that can be adapted to their needs and pace at a low cost.[36]

Engagement through gamification

CBTs are inspired by games and are particularly engaging (the social aspect, reaching goals, the reward and punishment system, identifying "vital" [37] behaviour, etc.). "Serious games" [38] can get employees involved in the training by immersing them in an engaging virtual world.[39 40 41 42]

This type of learning stems from motivation theories like **self-determination theory**. The latter is based on the notion of **intrinsic motivation** and suggests that our actions are largely determined by pleasure and personal satisfaction. It explains why games help participants adopt a particular

behaviour or a positive attitude toward something.[43] [44]

Increasing our sense of competency through simulation exercises

CBTs rely on cybercrime simulation exercises to promote engagement and participation by getting participants to interactively take part in realistic simulations.

This lets them assess their abilities while:

- **Improving their knowledge and skills** by learning to recognize the signs of a cybercrime.[45]
- **Understanding the impact of their decisions** thanks to quick feedback on what they learned.[46]
- **Developing an increased sense of self-efficacy**[47] having participated in deterring a threat in a realistic risk prevention simulation.

Simulation exercises are based on self-efficacy theories such as:

- **Social cognitive theory**, which addresses the importance of positive experiences in problem resolution. Whether someone will adopt a given behaviour can be influenced by how they perceive the consequences of their past actions (if their experience was positive, if they encountered difficulties, etc.).[48]
- **Protection motivation theory**, which holds that people decide how to act based on how threatening they perceive something to be. They assess their ability to stop the threat (self-efficacy) and weigh the costs and benefits of the behaviour they'd need to adopt to do so.[49] [50] In short, they need to believe that they're able to avert the danger and that they'll gain more than they'll lose by doing so.

CBTs are useful because participants can experience real cybercrime scenarios through them. They're encouraged to take a stance, recognize the consequences of their actions and realize that they're capable of adopting the required behaviour. This is evidenced by the fact that they feel in control when faced with a threat.[24]

Training that can be adapted to different participant profiles

The learning process in CBTs can be customized in a number of ways. Participants can:

- **Control how long training sessions last**.[23]
- Work on **different scenarios/topics** depending on their level at the company and prior knowledge.[15]
- **Develop their own cyber attack / cyber security scenarios** in line with their individual needs.[51]
- Easily switch between **several formats to access information** (text, audio, video) depending on what they're most receptive with.[52] [53]

However, CBTs also have limits that need to be addressed before implementing this kind of training:

- In the **self-learning** approach, participants can't talk to an instructor if they have questions or need more information.[47] [51] [54] [55]
- The **informational richness** of the medium and the **complexity of the format** can lead to cognitive overload.[56] This can cancel out the desired effect, that is, the participants' long-term retention of what they learn during the training.[45] [46] [53]
- **"Serious games" that are adapted for adult users** / company employees and that are educational enough without being overly complicated are **rare**.[57]
- This kind of training program requires **regular updates** because of how quickly technology is evolving—and therefore how quickly cybercrime threats are evolving.[58]

Improving how we assess awareness and training programs

Despite all the information in this briefing note, there's not enough empirical data to determine how effective these training programs really are. There are several training methods available, but there is hardly any research into their effectiveness.

There is also a lack of research on the impact of these programs on employees and the companies they work at. This makes it tough to evaluate their long-term impact on participants' awareness and behaviour and whether they've reached the initial goals of the training.[8 65 66]

More research is needed to look into how effective these programs are and how they can be implemented in companies.[27 67 68 69].

The rare studies that do assess the impact of cyber security awareness programs only do so on the basis of participant feedback, that is, on the basis of short-term subjective evaluations. There's still a lot of room for improvement.[27]

Practical advice for preventing data leaks

Using the two methods discussed in this article, businesses can increase their employees' awareness of information security issues, help them adopt safe behaviours and get them to follow information security policies (see the table in the appendix for a summary).

There are several key points to keep in mind when asking employees to adopt safe information security behaviours:

- Make sure that employees understand why adopting these behaviours is so important, for example, by showing them the consequences of their actions.[13 59 60 61]
- Combine training with continuous awareness campaigns so that employees can remember the key elements of what they learned in training.[30 62]
- Use visuals, short sentences and simple content so that participants can understand and remember the information more easily.[31 63 64]
- Motivate employees to do a task rather than assigning it to them. This makes it easier for them to integrate the desired behviours.[3 13 31]
- Complement the training program by encouraging your employees to adopt the behaviours they learned about, for example, by posting motivating messages on the company's internal portal or by asking your managers to visibly demonstrate the desired behaviours. [3 13]
- Give employees immediate feedback while they're learning so that they can make changes accordingly.[23 31 60]

References

1. Results obtained from companies that responded to a Statistics Canada survey in 2017.
2. Statistics Canada. (2017). Impact of cybercrime on Canadian businesses, 2017.
3 Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security, 56*, 70–82.
4. Technique used to trick someone into divulging confidential information.
5. Results obtained from companies that submitted their data incident data to Verizon in 2018.
6. Verizon. (2019). 2019 Data Breach Investigations Report.
7. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124–133.
8. Sending fraudulent emails to someone to get them to click a link.
9. Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2013). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy, 12*(1), 28–38.
10. Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276–289.
11. Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145–159.
12. Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security, 61*, 46–58.
13. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124–133.
14. See the Security Education, Training and Awareness (SETA) programs.
15. Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)* (pp. 62–68).
16. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS quarterly*, 757–778
17. McIlwraith, A. (2016). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.
18. Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432–445.

19. Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. *Information security technical report*, *14*(4), 223–229.

20. Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862–10868.
21. Ottis, R. (2014). Light weight tabletop exercise for cybersecurity education. *Journal of Homeland Security and Emergency Management*, *11*(4), 579–592.

22. Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014, June). Scene: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In *International conference of design, user experience, and usability* (pp. 229–239). Springer, Cham.

23. Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). MINDSPACE: influencing behaviour for public policy. *Institute for Government*.

24. Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015, July). Nudging towards security: Developing an application for wireless network selection for android phones. In *Proceedings of the 2015 British HCI conference* (pp. 193–201). ACM.

25. Acceptable behaviour in a given group.

26. The perceived social pressure to engage or not to engage in a behaviour.

27. Banfield, J. M. (2016). *A study of information security awareness program effectiveness in predicting end-user security behavior* (Doctoral Dissertation)

28. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523–548.

29. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78.
30. Konak, A., & Bartolacci, M. R. (2016). Using a virtual computing laboratory to foster collaborative learning for information security and information technology education. *Journal of Cybersecurity Education, Research and Practice*, *2016*(1), Article 2.

31. Inayat, I., ul Amin, R., Inayat, Z., & Salim, S. S. (2013). Effects of collaborative web based vocational education and training (VET) on learning outcomes. *Computers & Education*, *68*, 153–166.

32. The principal that to succeed as an individual you need to succeed in a group.

33. Laal, M., & Ghodsi, S. M. (2012). Benefits of collaborative learning. *Procedia-social and behavioral sciences*, *31*, 486–490.

34. Laal, M. (2013). Positive interdependence in collaborative learning. *Procedia-Social and Behavioral Sciences*, *93*, 1433–1437.

35. Roberts, T. S. (Ed.). (2004). *Online collaborative learning: Theory and practice*. IGI Global.

36. Furnell, S., Warren, A., & Dowland, P. S. (2004, July). Improving security awareness and training through computer-based training. In *Proceedings of the 3rd World Conference on Information Security Education* (WISE 2004). California: Monterey.

37. Holdsworth, J., & Apeh, E. (2017, September). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. In *2017 IEEE 25th International Requirements Engineering Conference Workshops* (REW) (pp. 111–117). IEEE.

38. Games whose primary purpose is something other than pure entertainment, like education.

39. Beckers, K., & Pape, S. (2016, September). A serious game for eliciting social engineering security requirements. In *2016 IEEE 24th International Requirements Engineering Conference* (pp.16–25). IEEE.

40. Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, *3*(1), 53–61.

41. Kulkarni, V. K. (2019). *Basic Cybersecurity Awareness Through Gaming*.

42. Raman, R., Lal, A., & Achuthan, K. (2014, March). Serious games based approach to cyber security concept learning: Indian context. In *2014 International Conference on Green Computing Communication and Electrical Engineering* (ICGCCEE) (pp. 1–5). IEEE.

43. Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230.

44. Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451.

45. George, J. F., Biros, D. P., Adkins, M., Burgoon, J. K., & Nunamaker, J. F. (2004, June). Testing various modes of computer-based training for deception detection. In *International Conference on Intelligence and Security Informatics* (pp. 411–417). Springer, Berlin, Heidelberg.

46. Cao, J., Lin, M., Deokar, A., Burgoon, J. K., Crews, J. M., & Adkins, M. (2004, June). Computer-based training for deception detection: What users want? In *International Conference on Intelligence and Security Informatics* (pp. 163–175). Springer, Berlin, Heidelberg.

47. The ability to adopt a target behaviour.

48. Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, *28*(8), 816–826.

49. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549–566.

50. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human Behavior*, *24*(6), 2799–2816.
51. Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*(1), 63–72.

52. Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing information security awareness at an Australian bank: a comparative study. *Information & Computer Security*, *25*(2), 181–189.

53. Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100.

54. Jacoby, R. (2005). Computer based training: Yes or no. *Journal of Health Care Compliance*, *7*(3), 45–48.

55. Hannum, W. (2001). *Web-based training: advantages and limitations*. Web-based training, Educational Technology Publications. New Jersey, 13–20.

56. The mental state of someone who receives more information than they can handle, resulting in their inability to retain the information in long-term memory.

57. To learn more about CyberCIEGE: https://my.nps.edu/web/c3o/cyberciege.

58. Roepke, R., & Schroeder, U. (2019). The Problem with Teaching Defence against the Dark Arts–a Review of Game-based Learning Applications and Serious Games for Cyber Security Education. In *11th International Conference on Computer Supported Education*. Heraklion, Crete, Greece
59. Ayyagari, R., & Figueroa, N. (2017). Is seeing believing? Training users on information security: Evidence from Java Applets. *Journal of Information Systems Education*, *28*(2), 115–122.
60. Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5/6), 352–357.
61. Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167–173.
62. Kim, P., & Homan, J. V. (2012). Measuring the effectiveness of information security training: A comparative analysis of computer-based training and instructor-based training. *Issues in Information Systems*, *13*(1), 215–224.
63. Chatzoglou, P. D., Sarigiannidis, L., Vraimaki, E., & Diamantidis, A. (2009). Investigating Greek employees' intention to use web-based training. *Computers & Education*, *53*(3), 877–889.
64. Mansurov, A. (2016). A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia. *Modern Applied Science*, *10*(11), 159.
65. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296.
66. Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), 1–39.
67. See the concept of external validity: The extent to which the results of a situation can be generalized to and across another group or context.

68. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008, October). Lessons from a real world evaluation of anti-phishing training. In *2008 eCrime Researchers Summit* (pp. 1–12). IEEE.

69. Tioh, J. N., Mina, M., & Jacobson, D. W. (2017, October). Cyber security training a survey of serious games in cyber security. In *2017 IEEE Frontiers in Education Conference* (FIE) (pp. 1–5). IEEE.

70. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–24for information security awareness and training. *Logistics Information Management*, *15*(5/6), 352–357.

61. Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167–173.

62. Kim, P., & Homan, J. V. (2012). Measuring the effectiveness of information security training: A comparative analysis of computer-based training and instructor-based training. *Issues in Information Systems*, *13*(1), 215–224.

63. Chatzoglou, P. D., Sarigiannidis, L., Vraimaki, E., & Diamantidis, A. (2009). Investigating Greek employees' intention to use web-based training. *Computers & Education*, *53*(3), 877–889.

64. Mansurov, A. (2016). A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia. *Modern Applied Science*, *10*(11), 159.

65. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296.

66. Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), 1–39.

67. See the concept of external validity: The extent to which the results of a situation can be generalized to and across another group or context.

68. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008, October). Lessons from a real world evaluation of anti-phishing training. In *2008 eCrime Researchers Summit* (pp. 1–12). IEEE.

69. Tioh, J. N., Mina, M., & Jacobson, D. W. (2017, October). Cyber security training a survey of serious games in cyber security. In *2017 IEEE Frontiers in Education Conference* (FIE) (pp. 1–5). IEEE.

70. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–24

Appendix

Performance criteria	Collaboration group		Computer-based training	
	Included	Key features	Included	Key features
Awareness	✓	Participation Identification Accountability	✓	Range of media/formats Behaviour assessment Self-efficacy
Change in behaviour	✓	Active discussion Collective reflection Interaction with instructor	✓	Taken on the computer/Internet Simulation
Compliance with company policies	✓	Sharing knowledge and experiences Engagement Social norms	✓	Situation-based simulation Feedback Self-efficacy
Knowledge acquisition	✓	Information acquisition through discussions	✓	Information acquisition through simulations
User satisfaction	✓	Socializing with colleagues and the instructor	✓	Motivating and engaging gamification
Benefits	✓	Social influence Organizational culture Sharing knowledge and experiences	✓	Profitability Control of pace Customizable Large-scale distribution