computing research

RESEARCH PAPER

Cyber security training: a box ticking exercise, quickly completed, even more quickly forgotten?

December 2018

Sponsored by

mimecast®

CONTENTS

Executive summary

Surveys across global businesses are unanimous in their conclusions: human beings represent the single greatest cyber security risk. For all the perils of automation and connected technologies, human error is responsible for as much as 95 per cent of security breaches.

At the same time, the source of most security risks is also human agency: the malign actors aiming to steal data, divert finances and disrupt companies' activities through multiple cyber tricks, from phishing to ransomware to hacking. These security risks depend upon the vulnerability of employees, whether from inattention, deception or theft.

Combatting this human problem requires human-focused solutions. There is only so much that firewalls and other security architecture can achieve, when systems, that are designed for people to use, must be fortified.

One answer is to invest in training programmes, so that employers can gain greater confidence in their colleagues' capabilities: to understand the threats, to take precautions against cyber threats and to act wisely when threats present themselves.

Computing surveyed 150 UK IT decision makers comprising Chief Information and Technology Officers, IT managers, Security and other IT professionals – each representing organisations with over 250 employees – to determine the level of cyber security training and awareness in their businesses.

Research areas included:

- Measures that organisations can take to protect themselves against email-borne cyberattacks
- Activities where employees are most likely to make a security mistake
- Most valuable security concepts for employees to understand
- Frequency of employee training on cyberattacks
- Types of cyber security awareness training, their costs and development processes
- How employees respond to cyber security training
- Employers' interest in focused training and remediation measures

Research highlights included:

- Staff training ranked far above improved business processes or increased investment in technology (scoring 355 against 267 for processes and 214 for tech investment)
- Casual, inadvertent behaviour such as not locking a computer screen was viewed as the most serious security risk by employees, ahead of poor password hygiene and cloud storage
- Valuable security concepts were lead by strong password creation, boosting physical security and limiting personal use of company cloud storage systems
- Almost a third of respondents' organisations provide annual security training, yet more than a fifth (22 per cent) only do this 'after a big event or when a threat is detected'.
- Online tests, with formal questions about security threats, are the most popular form of security training. One in eight respondents provide no training at all
- 62 per cent of respondents use third party vendors to provide awareness training and 59 per cent spend at least £10 per employee per annum
- The great majority (82 per cent) of respondents felt security awareness training made a difference to their organisations, with 50 per cent saying that employees responded 'quite well' or 'very well' to the process
- Nevertheless, of respondents' concerns over training, the most common feeling was that 'training is seen by employees as a box-ticking exercise'

The primary importance of training

Asked to rank the importance of training staff in the risks from cyberattacks and how to protect themselves and their organisations, against improving business processes to be less susceptible to attack, or increasing investment in technology and cloud services, the overwhelming response was to rank training as number one.

This demonstrates the crucial role of human agency in technology decisions: however good an organisation's processes are, or however sophisticated its cloud services, if the people involved are insufficiently trained or aware of risks, there is an ever-present danger.

Respondents' concerns over training standards also reflect growing alarm throughout industry over the dearth of security experts and the increasing risks of non-compliance with regulations such as GDPR, introduced in May 2018.

Where do mistakes happen?

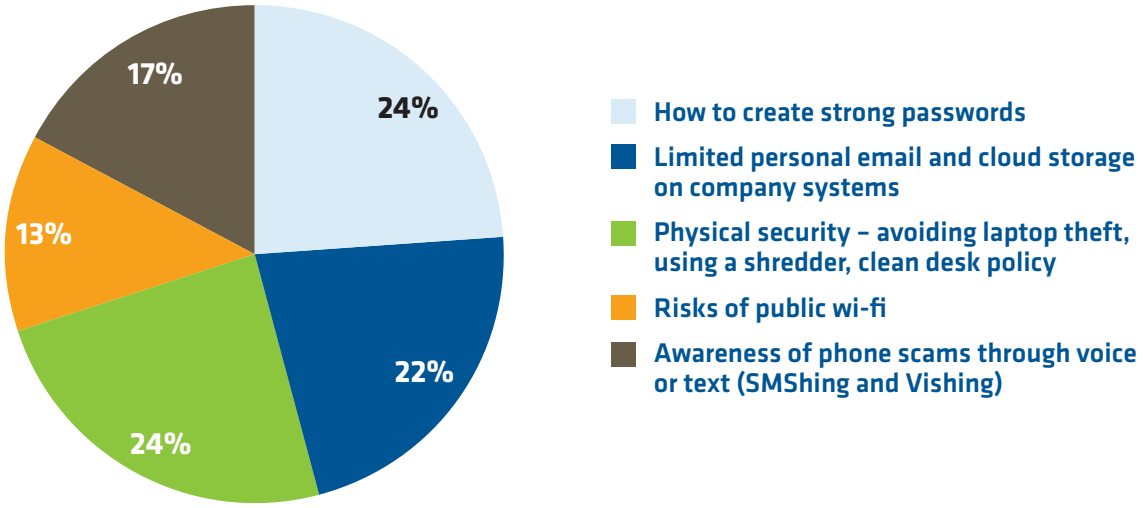
In a list of six options, respondents chose 'inadvertent data leaks' – which included not locking their screens, leaving confidential papers on their desks and leaving devices unattended – over five other kinds of office behaviour, from poor password hygiene (the second most popular choice) to cloud storage, browsing the web, visiting social media and personal emails.

You could argue that all of these choices involve inadvertent behaviour: employees surely wouldn't browse websites or use social media deliberately trying to cause a security problem. But the carelessness of these data leaks is more easily identified as a problem, since it can be physically observed and witnessed, and is more or less outside employers' control.

Of the other five options, password hygiene and access to cloud storage are issues that good employers should regulate and oversee, so if employees make errors in these areas, employers must take a share in the responsibility. Even email security, social media activity and website browsing are within the remit of most organisations' IT department to secure.

A further question, asking which security concepts would be most valuable for employees to remember, elicited a similar range of answers. Physical security, defined as 'avoiding laptop theft, using a shredder, clean desk policy' came above various more tech-focused answers such as strong passwords, limiting personal email and awareness of mobile device scams.

Fig. 1 : Beyond phishing, which security concept do you think would be most valuable for your employees to remember in order to keep them and the organisation secure?



In summary: *managers view physical carelessness – which is harder for them to oversee – as one of the biggest threats to cyber security.*

What training is offered?

In our survey, 99 per cent of respondents made a positive reply in answer to 'how frequently do you train your employees to spot cyberattacks?' Yet for 22 per cent of these, the answer was 'Training is usually ad-hoc, usually after a big event of when a threat is detected'.

This reactive, passive approach to cyber security by almost a quarter of respondents is clearly alarming, and explains why so many companies register shock and disbelief when they suffer major cyberattacks. If there is no preparation, no formal plan for prevention and no awareness programme other than 'after a big event' for so many businesses, it is amazing that more damage hasn't already occurred.

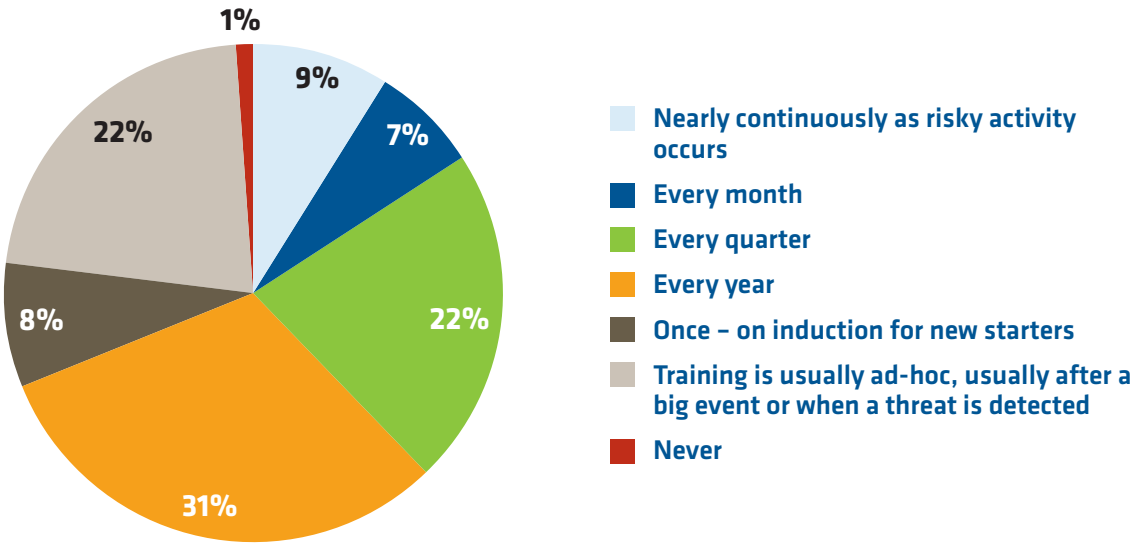
By contrast, 9 per cent of respondents have a continuous programme of training, a further 7 per cent conduct training every month, 22 per cent every quarter and a further 31 per cent annually, so there is at least an ongoing effort to deal with the issue among 69 per cent of the survey cohort.

Qualitatively, training comprises largely online resources: the most popular – used by 58 per cent of respondents' organisations – is a 'formal online test to learn about threats and prompts questions to respond to'. This has the advantage of being interactive, requiring some activity from the employee, as do the 'interactive videos highlighting best/worst practices to keep in mind', which is the second most popular option, chosen by 41.3 per cent of respondents.

Lower down the scale of training methods are lists of tips for employees to read and prompts to accompany online links, noting whether they are safe. You might hope and expect that companies would provide all of these kinds of assistance to employees, clearly they don't.

Whereas only 1 per cent said they 'never' train employees to spot cyberattacks, a full 12 per cent chose the option 'My company doesn't provide any training' in this separate section – arguably leaving more than one in ten organisations at far greater risk of breach.

Fig. 2 : Approximately, how frequently do you train your employees to spot cyberattacks?



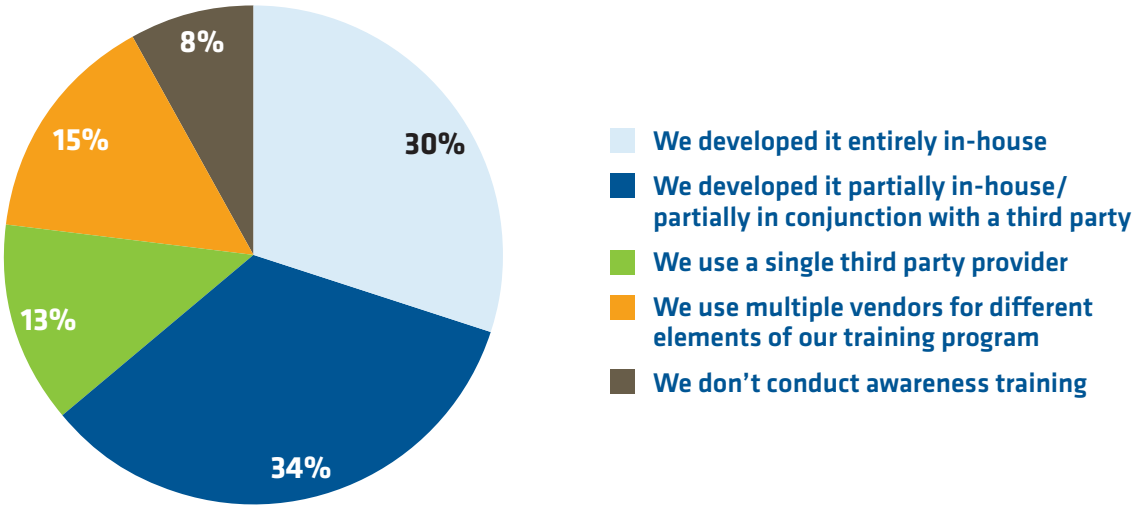
In summary: *there is a remarkable spread of responses across the respondent group over training to identify cyberattacks, from constant readiness to neglect. Many organisations prioritise interactive training, although 12.5 per cent do none at all.*

How training is developed

Of the 150 respondents to this survey, just under two thirds (64 per cent) either develop their own cyber security awareness programme or in partnership a third party. This shows a strong self confidence among respondents to deal with these issues from within their own management ranks – given some external help. The majority worked with some outside provider, 13 per cent of these using a single supplier and 15 per cent using multiple providers.

We are unable to see how these figures have moved over time, but one may assume that the number and proportion of outside agencies has risen in recent years, as the variety and severity of cyber security risks has increased.

Fig. 3 : How did you develop your awareness training program?



Equally, the annual amount spent per employee has almost certainly risen. In our survey, the cost varied from 'nothing' (12 per cent of respondents) to 'More than £75 per employee' (7 per cent), with the average amount resting somewhere around £20 per employee.

We can easily see these amounts rising steeply in future, as the potential penalties of non-compliance with GDPR (4 per cent of annual turnover or €20 million) combine with greater awareness of the loss of revenue and reputation that cyberattacks can cause.

In summary: *most respondents employ third party providers to assist with cyber security training and the great majority invest in it, although the degrees of engagement and investment vary widely.*

How employees respond to training

Exactly half of respondents reported that their organisation's employees responded 'Quite well – There is definitely an effect, but it's not as widespread as we would like' (28 per cent) or 'Very well – We notice definite, positive changes in behaviour' (22 per cent). A further 32 per cent agreed that the training made a difference 'but human error still runs high'.

The negative responses ('Badly - Training makes little or no difference' – 1 per cent, and 'Not well – There seems to be little discernible take-up of practice' – 10 per cent) are therefore hugely outweighed by the positive and the partially satisfied. The likelihood is that those who registered poor responses were those who spent least time and least resources on training, meaning that the two issues are self-reinforcing. A further 2 per cent don't collect any feedback to determine effectiveness and 5 per cent (in response to this question) don't conduct security training.

Respondents were posed a second question concerning employee responses. This one comprised entirely negative options, from 'Training is expensive' to 'There is little to no feedback as to the effectiveness of training', with a further six downbeat options in between.

From this grim list, respondents decided that 'Training is seen by employees as a box-ticking exercise' was the closest to their experience, followed by 'Training is quickly completed and even more quickly forgotten'. Respondents clearly felt herded into the middle ground of 'somewhat agree' and 'somewhat disagree', or yet further away from expressing an opinion, into 'neither agree nor disagree'.

In summary: *the wide spread of employee experiences show that while many are satisfied, for some organisations the jury is firmly out on the effectiveness of training, and many believe there could be improvement.*

Conclusion

The lessons from this survey are clear: training is a key factor in combatting cyber security concerns and identifying cyberattacks and raising awareness among employees. The dangers from physical carelessness and inadvertently risky behaviour outweigh the risks from employees' use of technology. Although the majority of organisations train their employees and invest in this training, a significant minority neglect to do so.

Interactive training methods are the most popular, and third party agencies are commonly used to develop training programmes. Most employees react positively to cyber security training, although a 'box-ticking' mentality is common.

In a final question, respondents were asked whether they would value an employee risk score, to determine the specific risk of employees. To this, 45 per cent responded that they were 'very interested' (11 per cent) or 'somewhat interested' (34 per cent), while the remaining 55 per cent were unsure, not very interested or not at all interested.

Since the great majority of respondents already had cyber security training programmes in place, it's interesting that they are nevertheless interested in an employee risk score.

Humans, after all, are often the weak link when it comes to cyber security.

About the sponsor, Mimecast

Mimecast develops cyber resilience strategies for business. The company helps organizations adapt by leveraging third?party threat intelligence, continually assessing and deploying leading technologies, conducting ongoing threat analysis, automating remediation services, and delivering inline user education to help employees be more aware and cautious.

For more information:

Visit: www.mimecast.com

Mimecast Awareness Training

Mimecast Awareness Training solves your organization's vulnerability to human error by combining effective, modern training techniques with predictive analytics to reduce the security risk arising from simple employee mistakes made by well-meaning people. We change employee behavior effectively by showing employees what to do, engaging with them in a way that encourages them to care enough to improve and then respond appropriately when it matters. Its cyber training done right – made fun, delivered fast and proven effective.

Learn more or schedule a demo:

Visit: www.mimecast.com/awareness

mimecast®