CASE STUDY: SECURITY AWARENESS TRAINING

Simplifying security awareness training

BACKGROUND

In recent years, employees have become the front line in protecting businesses from information security risks. However, criminals are wily and the likelihood of breach from an untrained employee has never been so high. Standards writers and regulators have recognised the increasing risk, and have been quick to mandate security awareness training programmes.

Security awareness training is easier said than done. Many organisations lack the historical investment in training platforms and specialist subject matter expertise. Most organisations have large, dispersed workforces and traditional classroom-based training is either not practical or fit-for-purpose. Organisations have quickly found that a new training approach is required.

CHALLENGE

Our client accepts payment cards across various payment channels (in-store, online, contact centre). They are also a service provider, delivering co-location and infrastructure services to merchants. They had immediate challenges in meeting or demonstrating compliance in:

- Implementing a formal security awareness programme to make all staff aware of the importance of cardholder data security
- Educating staff upon hire and at least annually
- Training staff to be aware of suspicious behaviour and to report tampering or substitution of devices that capture payment card data
- Training developers in secure coding techniques

Considering the nature of the client's business, it was evident the task ahead was much bigger than training content and logistics. They needed to overcome a whole new range of challenges beforehand, including:

- Moving teaching into long-term memory
- Delivering on-demand, repeatable training
- Making regular content updates
- Tailoring training to various roles
- Training large and increasingly dispersed workforces
- Making security part of the organisation's culture
- Managing progression, testing comprehension and creating auditable evidence
- Making training more affordable than previous programmes

Moving teaching into long-term memory

Traditional classroom training is appropriate for many subjects, however much data security training is technical, dry and un-engaging. It is often created by people who are not experts in either data security or training. As people typically only retain around 10 per cent of information from classroom-based training, and the risks associated with storing, transmitting and processing information are now so high, our client needed an alternative. The training needed to be quick, relevant and fun, helping it to be retained within the employee's long-term memory.

Delivering on-demand, repeatable training

To meet the needs of varying security standards, client contracts, employment of seasonal and transitory staff, the client required high-quality, specialist training content to be available throughout the year and on demand. This improves the boarding process for new joiners, and ensures that untrained staff are not opening the organisation to unnecessary risk.

Making regular content updates

The information security and regulatory landscape is constantly evolving. The client knew that threats, standards and regulations change with increasing frequency. The training content would therefore need to be updated with a similar frequency, and by specialists with much greater understanding than those from a single business area or discipline.

Tailoring training to various roles

Information security is relevant to employees from all areas of the business, so the training programme needed to reflect this. The content needed to address each in a way that was appropriate to their business role. This required the use of different delivery mediums and courses, and content written by subject matter experts, rather than by the in-house IT department or a training generalist.

Training large and increasingly dispersed workforces

As many retail businesses, our client employs a number of temporary, part-time and seasonal staff. For larger organisations, the logistics of training thousands of staff across multiple locations and job roles, whilst managing the costs to the business of doing so, is extremely complex. Training people quickly upon hire and without requiring large amounts of time away from their day jobs, is critical. A training platform or portal would therefore be required to make training content available regardless of work shift patterns or location.

Making security part of the organisation's culture

Embedding security into organisational culture is not a 'one and done' activity. Our client recognised this and wanted the training to support a business plan to drive cultural change. The challenge was how to reinforce the training across the business with messaging that was instantly recognisable as part of the training. This would remind people to 'live' security, keeping the messages front-of-mind at all times.

Managing progression, testing comprehension and creating auditable evidence

Our client not only needed to demonstrate that they had trained all staff at least annually. Staff also had to evidence effective comprehension and that learnings had been translated into their day-to-day roles. Both these aspects are typically verified by a QSA as part of a PCI DSS audit. The client wanted a way to assess an initial understanding of information security, oversee that training was being conducted, measure comprehension and record auditable evidence of this.

Making training more affordable than previous programmes

As many organisations, our client's training department was expected to do more with less budget. The security awareness training solution had to increase training provision without increasing the overall budget requirement proportionately. In short, the cost of training per head needed to decrease, not increase.

OBJECTIVE

The objective was to simplify security awareness training for a complex business. This would make achieving and maintaining compliance with prescribed standards (e.g. PCI DSS, ISO 27001) easier for our client, and help them make best use of their scarce training budget.

SOLUTION

Blackfoot's training solution met all the client's objectives. Following an initial scoping exercise, we quickly matched these needs against elements of a mature Blackfoot offering. This included assessment services, memorable training content, supporting materials and a training platform, where staff participation and comprehension could be audited as evidence towards PCI DSS and ISO 27001 compliance.

To overcome the problem of moving training from the short to long-term memory, Blackfoot created a comprehensive suite of 2-3-minute security awareness training videos. These were written and designed by industry experts to be short, sharp, memorable and fun.

As the training content was available via subscription on an unlimited basis, it could be replayed as many times as required to maximise retention. The videos were also developed to be relevant to employees personally, so they could apply the learnings outside work (e.g. protecting against e-mail scams and identity theft). In this way, we secure the employee to secure the employer.

A poster campaign throughout the company reinforced critical security messages and kept training content top-of-mind. Poster locations and messages were changed and refreshed regularly.

To overcome the problem of updates, the training content was provided under an affordable subscription model. This included updates when standards were changed or the security landscape evolved. With no limit to the updates, our client could provide relevant and up-to-date training to all employees at any time.

To ensure training content was correctly focused, the training service started with an evaluation exercise. This identified mandated training requirements and mapped audiences and requirements to modules that included:

- Core cyber security awareness
- Face-to-face payment security
- MOTO payment security
- Handling personal data
- Additional security for home and mobile workers
- IT operations and IT support
- Software development teams
- Cyber security executive briefing

Following this initial mapping, we undertook a further exercise to consider which of the available mediums best suited the audience. In the majority of cases, training was delivered via video content. However in specialist areas, such as software development, gamification was used to engage developers in learning through play. By using the Blackfoot/OWASP Cornucopia card game, software developers were able to trade their understanding of security in development in a fun and memorable way. Similarly, business executives were engaged with relevant, topical and classroom-based workshops that focused on issues such as business risk, reputational damage and the impact of a breach.

The deployment of a learning management system often takes weeks or months, delaying the delivery of training. Blackfoot provided access to an alternative, fully-featured learning management system (LMS), which could easily be configured with user accounts, learning paths, content and quizzes. Deployed in minutes rather than months, the system was able to serve content to employees regardless of location or department.

The LMS issued trainees with certificates once they had passed their training. It also provided managers with oversight on inactive accounts, course status and auditable information for compliance assessors. Blackfoot can also supply content in an industry-recognised format that fits a range of LMS.

Making training affordable was a key consideration for our client. Providing reusable video-based content delivered direct to users (in the workplace or at home) significantly reduced the overheads of travel and lost productivity. A subscription model based on the number of employees cut costs compared to traditional training methods. The client could also predict future training costs. The all-in cost also included upgrades, training workshops, and an assessment of improvement through phishing exercises.

RESULTS

The training not only improved employee security awareness, but also met compliance standards and best practice requirements, while delivering massive productivity and cost savings to the client.

80 per cent of in-scope staff were trained within three weeks of roll-out. It took approximately one hour to train each of 500 employees, compared to the 7.5 hours per employee required for an all-day training course. This delivered a productivity saving of 6.5 hours per employee, or 3,250 hours across the business in the first year. Additionally, the client saved operational overheads of delivering multiple classroom-based courses.

The client has since ordered a two-stage phishing e-mail campaign to validate and measure the success of the training.

FOR MORE INFORMATION

Blackfoot's security awareness training is commercially available and has been adopted by clients in the financial services, telecoms, retail, food and beverage, and leisure industries.

To find out more about Blackfoot's security awareness training or to receive a quotation, please contact your Blackfoot account manager.

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >
ASSESS >
ASSURE >