Information Security Awareness Survey 2008

Prepared by SAI Global
Security Awareness: Measuring Attitudes, Knowledge and Behaviour

Results of The SAI Global Benchmarking Survey 2008

Current Security Awareness Trends

Over the last five years SAI Global has seen the demand for security awareness training grow – with increasing numbers of companies approaching us for products and solutions in this area. Our clients understand that addressing the human element of information security through innovative and engaging security awareness initiatives is a vital part of their security architecture.

The CSI 2008 survey supports the increased uptake in security awareness initiatives by organisations. It concluded that just 18 percent of companies admitted that they don’t use awareness training, “implying that 4 out of 5 respondent organisations do in fact engage their employees about security risks and appropriate handling of sensitive data”.

Despite companies being more pro-active generally about the take-up of security awareness training, the CSI survey results also identified that spending on training still remains low – the majority of organisations spend less than 1 percent of their security budget on awareness training. It also appears that companies are doing little to measure the effectiveness of security awareness. For the first time this year the CSI survey asked organisations what measures they had adopted to gauge the effectiveness of their security awareness training programs. The results concluded that: “many of the respondent organisations (32 percent) make no effort to measure the effect of this training on the organisation”. Without these important metrics it is easy to see why many companies appear cynical about spending money on security awareness training.

Extending The Focus Of Security Awareness Training – Measuring Attitudes, Knowledge And Behaviour

The question is no longer ‘Should we educate users?’ but ‘How do we make sure that our security education is effective and results in meaningful behavioural change that addresses the persistent and serious risk of human error?’ SAI Global’s experience in the security awareness market leads us to believe that much of the existing security awareness material being used by organisations focuses too heavily on delivering facts to learners about security policy. Our philosophy is, that in order to be effective it is important not only to address the knowledge of users, but also their attitudes and behaviours.
As the Venn Diagram above shows, An organisation’s overall security position is enhanced when the attitudes, knowledge and behaviours of users are aligned with security objectives and requirements.

**Attitudes** - users’ attitudes are important because unless they believe that security is important users are unlikely to work securely, irrespective of how much they know about security requirements. Attitudes give a strong indication of an employee’s disposition to act.

**Knowledge** - is important because, even if a user believes security is important, he or she cannot carry that intention into action without the necessary knowledge and understanding.

**Behaviour** - finally, no matter what individuals believe or know, they will not impact security unless they behave in a secure fashion.

From a user perspective, security lies in the overlap of attitudes knowledge and behaviours. If an organisation wants to know if their security awareness training is effective, they need to measure the impacts on these three elements.
The Benchmarking Survey

SAI Global conducted a benchmarking survey in order to help organisations assess current levels of attitudes, knowledge and behaviour towards information security, and to provide them with a benchmark against which to measure the impact of future awareness initiatives.

How We Approached It

SAI Global invited information security professionals to participate in the first SAI Global information security benchmarking survey. Many professionals saw a real value in learning more about their employees’ view of information security and how it affects them. Ten companies chose to participate in the survey and circulated a short 15 question online survey to their employees. This provided a sample of 1282 total respondents. For this report SAI Global has aggregated all results to provide a general overview of employees’ attitudes, knowledge and behaviour in relation to information security. The companies who participated were also provided with their own unique survey results compared against the aggregated data.

An Overview of the Main Conclusions

In the current climate of high profile security breaches, it is hardly surprising that respondents to our survey had broadly positive attitudes to information security. The majority acknowledged its importance to business and recognised that everyone in an organisation has some responsibility for information security. More concerning, however, is the evidence that a significant minority of respondents were unwilling or unable to put these positive attitudes into practice. So, although 95% of respondents believe security is important around one quarter had not received any information security awareness training, and more worryingly one fifth said that they did not know how to report a security incident. Almost a quarter did not think it was appropriate for employers to monitor email and internet use, and 31% felt that information security requirements interfere with their ability to get the job done.
KEY FINDINGS

Attitudes

Respondents overwhelmingly (95%) see the connection between information security and the achievement of business objectives. This could, in part, be a result of recent high-profile security incidents that have generated a lot of adverse publicity for public and private organisations.

I believe that information security is an important factor in achieving our business objectives

Despite acknowledging the importance of information security in achieving business objectives, nearly a third of respondents overall felt that security requirements interfered with their ability to get the job done. Possibly indicating that more effort needs to be made to forge the connection between security policies and protection of organisations and their employees.

Information security requirements may interfere with my ability to get the job done
Although respondents agree that security is important to their businesses, we see a degree of resistance to security practices when there is a potential impact for individual employees. So, nearly one quarter of all respondents disagree that their employers should monitor their use of email and Internet – employees are still skeptical about being monitored and companies still have some way to go to get ‘buy-in’ to this practice.

Employers should monitor how employees use e-mail and the internet

Employees overwhelmingly agree (97%) that information security is everyone's responsibility within an organisation. This would suggest that any future security awareness or training initiatives should be targeted at all employees, including the board, managers, temporary staff and contractors, with the overall goal of creating a security conscious workforce – from the top-down.

Every individual in the organisation is responsible for information security

SAI Global Information Security Awareness Survey 2008
Knowledge

Worryingly, only 75% of respondents said they know how to **recognise** a security incident and only 64% said they know how to **report** a security incident. This represents a missed opportunity in terms of putting positive attitudes into practice and also demonstrates a clear knowledge gap that needs to be addressed by organisations. Core awareness initiatives should not only promote why reporting incidents is important, but also provide clear information on how to report an incident. In addition, reinforcement tools (posters, email campaigns etc.) could be used to remind employees of the incident reporting process with the goal of keeping incident reporting processes front-of-mind.

Interestingly nearly 1 in 5 (19%) do not know where to find their organisation’s security policy and a further 14% selected neutral when asked this question. Companies need to address this issue to ensure that employees have access to this information when they need it, and importantly, are aware of where they can find it.
In addition, further results showed that 16% of respondents disagreed that they know where to go for help relating to security incidents, while 14% disagreed that they have read and understood their organisation’s information security policies. Companies clearly need to place more focus on providing employees with support and advice relating to security issues/incidents – and this should be promoted in all security awareness initiatives.

**I know where to go for help and advice relating to information security issues**

- Strongly agree: 582 (45%)
- Agree: 327 (26%)
- Neutral: 168 (13%)
- Disagree: 183 (14%)
- Strongly disagree: 22 (2%)

**I have read and understand my organisation’s information security policies**

- Strongly agree: 664 (52%)
- Agree: 254 (20%)
- Neutral: 187 (15%)
- Disagree: 154 (12%)
- Strongly disagree: 23 (2%)
Behaviours

Perhaps not surprisingly, most respondents agree that they follow security policies in their work (77%) and similarly the majority believe that security policies are followed in their departments and that they are encouraged to work securely by their managers (73% and 72% respectively). In each of these categories though, the proportion of neutral responses was relatively high and there was even a small minority (of around 6% in each case) who actively disagreed. This perhaps indicates that we have some way to go in terms of ensuring that security is high on the list of business priorities and shows scope for further engagement of management in promoting positive information security best practice.

I always follow information security policies in my work

I am encouraged to work securely by my manager
Organisations still have some way to go in ensuring that information security awareness training is provided for all employees. Only 63% of employees were in positive agreement that they had received training. Over one quarter of employees (37%) did not agree, and could pose a security risk to companies. Training initiatives need to be more robust in ensuring full coverage throughout the organisation – including new starters, contractors and third parties.

78% of respondents would report behaviour that they thought jeopardised information security. Although this is a broadly positive result, again there were a high number of neutral responses (19%). There may be some overlap here with the respondents who said that they did not know how to report a security incident and again positive reinforcement of the incident reporting process should help to ensure that more employees provide a positive response in the future.
Join SAI Global for the 2009 Benchmarking Survey...

The 2009 Benchmarking Survey will be launched at Infosecurity Europe 2009. Companies who would like to participate should contact SAI Global on: info.emea@saiglobal.com or visit the SAI Global Stand H85.

Please note: to qualify organisations will need a minimum of 50 end-users to participate in the email survey.

About SAI Global

At SAI Global we work with your organisation to build a positive compliance culture. Using our international experience, we deliver effective solutions to help you manage business risk, achieve compliance and promote ethical behaviour.

Our Approach

We offer a flexible range of risk and compliance solutions and services, which engage staff at all levels of your organisation.

- **Know** what affects your business
  
  Our global newsfeeds keep you up-to-date with the regulations, standards, policies and trends affecting your business

- **Communicate** and train
  
  Our training and awareness solutions can be tailored to meet your requirements to bring about long-lasting and positive behavioural change amongst your employees.

- **Evaluate** and report on your compliance programs
  
  Our GRC software provides you with a platform to evaluate and report on your organisation’s compliance, risk and ethics policies and procedures.

Our solutions

We offer a range of solutions and services in risk areas such as:

- Financial Crime (including Anti-Money Laundering and Fraud)
- Information Security
- Data Protection & Privacy
- Ethics and Compliance (including Code of Conduct)

For further information call us on +44 (0)1926 854111 or email us at info.emea@saiglobal.com. Alternatively visit our website at www.saiglobal.com/compliance