How to create a security culture

Cultivating a secure workplace from the inside out

SnapComms
Get Employee Attention

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Creating a secure and safe working environment has become an essential priority for employers. Cyber-attacks, terrorist activity and even inadvertent employee actions feature all-too-frequently in the media. No organization or individual is immune.

Effective communication and education for staff so they understand the risks is central to developing a robust, security-conscious culture. But this has been highlighted as one of the biggest challenges faced by employers.

According to SANS 2015 Security Awareness Report, survey respondents cited they lack the training, resources and support to create an engaging staff security awareness program.

So how do you get staff to sit up and take notice about security? To recognize their behavior can be the first and best line of defence in this new world of threat? What can you do to help employees identify the danger signs and mitigate risk?

And how do you maintain a culture so that security remains front and centre for staff, long after the classroom training?

This white paper has been produced to help organizations implement an ongoing security framework for all staff through better communication and training.

Increasing attention on security

People, facilities and assets have been the traditional focus of workplace security. But recently, the nature and extremity level of risk have surged, specifically within the scope of data security.

The digital revolution has created a Pandora's box of cyber threats, with powerful attacks able to paralyze a company.

Some of these include:

• Insider threats – disgruntled, careless or departing employees with privileged access to networks, data centers and databases can cause serious damage.

• Mobility and BYOD – a mobile workforce increases corporate vulner-ability, particularly when expensive digital devices are lost or stolen, and confidential information is leaked.

• Social engineering– this involves tricking people into breaking normal security procedures. Phishing (fraudulent emails disguised as legitimate emails) and baiting (inserting malware-infected devices, such as a USB) are just two of the traps employees can easily fall into.

These threats – plus those we don't even know about yet – are jeopardizing businesses. Customers want assurances their data is safe. Employees want assurances their personal information is safe.

This explains why 75% of enterprises' information security budgets are estimated to be allocated for fast detection and response approaches in 2020– up from less than 10% in 2012.

Security is now fundamental to business operation and survival. It's becoming embedded within every business practice, rather than regarded as a separate silo.

No longer is it seen as a single issue that can be parked at the IT department's door.

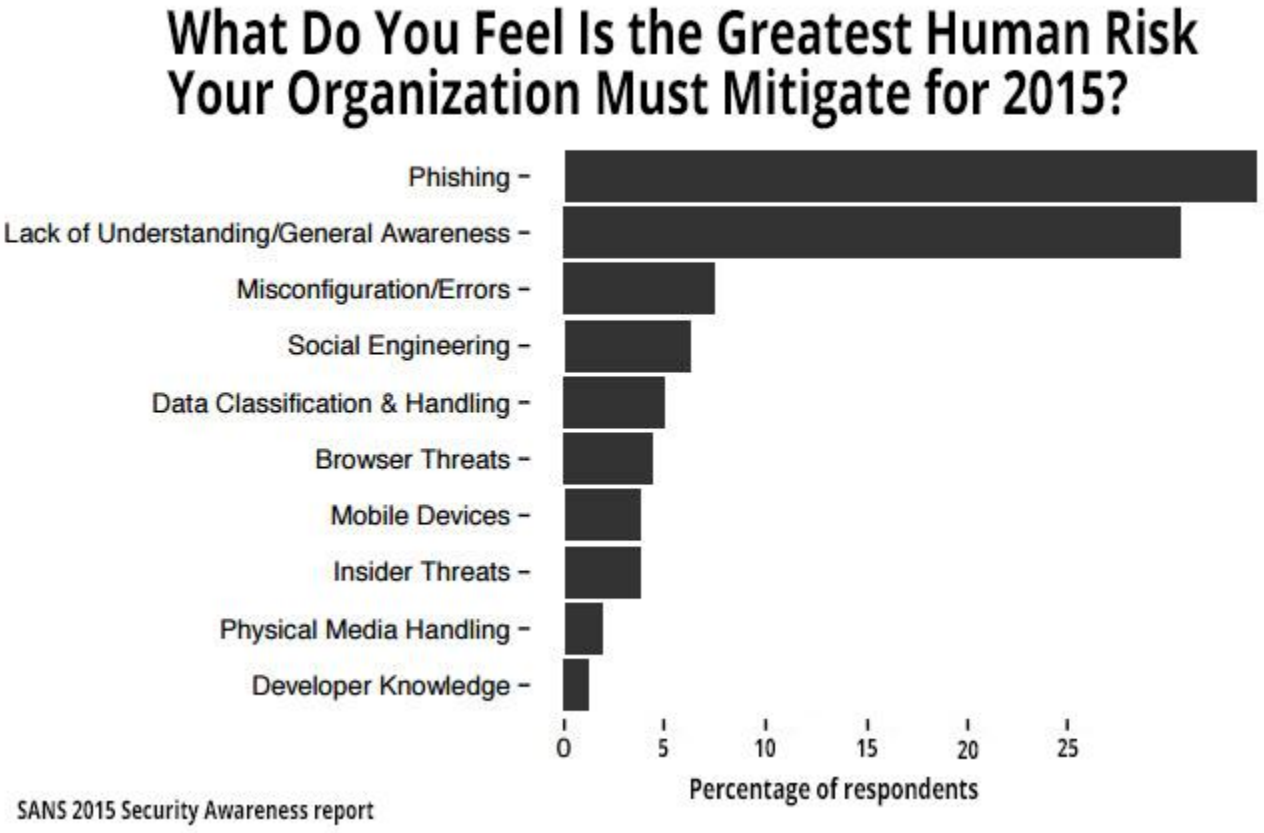
The biggest threats

The first step to mounting a good defense strategy is to know what the threats are.
Phishing is the number one human risk according to SANS 2015 Security Awareness report. This is the fraudulent practice in which a 'phisher' masquerades as a reputable entity (such as a bank) and induces individuals to reveal sensitive information such as bank details and passwords in order to steal money.
The second risk identified by the survey respondents is the lack of understanding and general awareness on the need for security.
The good news is that a well thought out internal communication program can address these.

No phishing here!

With some basic training, staff can easily detect the tell-tale signs of a phishing scam. For example, by hovering over a URL link embedded within in an email reveals the actual hyperlinked address. If it's different from the address displayed, the message is likely to be malicious.

Poor spelling and grammatical mistakes are other telling signs of a scam email, as are requests for logins and passwords.



Ignoring the signs, or an honest mistake?

Many organizations mistakenly believe that their biggest risk of a cyber-attack is from an external source.

The reality is most security incidents come from inside.

For some staff, turning a blind eye on a wrongdoing may seem an easier path than whistle-blowing. Employees are not always sure of how and who to report an act of misconduct to. Typically, they don't like to rock the boat, and worry they may somehow be implicated, or their own reputation damaged. Ironically, their inaction could be regarded as unethical, leading to disciplinary action.

Adopting a code of conduct outlining the procedures for reporting unethical behavior is becoming the norm. More than half the states in the US have whistle blower laws; these also prohibit retaliation against those reporting the incident.

Unintentional disclosure of sensitive information or mistakenly forwarding an email can also wreak financial, reputational and organizational damage.

These types of data privacy breaches can be costly. Data security experts estimate approximately $5.9 million is the average organizational cost of a data breach.

But unless staff are properly trained on correct security measures, and know how to recognize and avoid a security incident, the risk lays squarely with their employer.

Never has it been so important for employers to step up and take decisive action for deterring threats.

4.5 million

smartphones were lost or stolen in U.S. in 2013.

That's up from 2.8 million the year before. Over half were unable to get their smartphone back.

Communication timetable for employee training

An effective internal communication program comprises of three stages. Here is a recommended timetable for communicating through each stage.

• Stage 1: Nurture

Weeks 1-2

This 'nurture' phase is initially about grabbing people's attention, alerting them to problems, and warming them to be more receptive to behavioural-change (stage 2).

A great way to kick start a nurture campaign is to launch with some startling facts. For example: *There are 100 million phishing attacks every day – could you be next? Or*

'Almost every American has been affected by a data breach in 2015 – find out what this means to you.'

Create scenario-based content. This will spark debate amongst co-workers, get them thinking and talking about their own security behavior, and consider the consequences.

A series of these messages developed and released in short, sharp bursts are designed to make an impact and build momentum quickly.

As much as your budget will allow, employ multiple communication formats to deliver the message – not just email. This could include screensavers, noticeboards, desktop pop-ups, and scrolling messages on screen.

• Stage 2: Educate

Weeks 3-4
(with ongoing reminders)

The 'educate' phase is the crux of the campaign, whereby the key behaviors you're trying to promote are relayed. These should be ongoing and delivered across a variety of coordinated channels, from classroom training, presentations to digital assets. Invite staff to attend a workshop, classroom training, and/or online session. At these events, illustrate common scams and security breaches with real or hypothetical cases. Tip: Videoing these sessions is a good idea, as they can be edited and repurposed for reminder training later.

As the education stage is ongoing, it must also include reinforcement and reminder messages: the repetition effect helps with habit formation, memorization, and comprehension.

Straight after these sessions, follow up with 'key messages to remember'. Use screensaver messaging as passive reminders. Also consider running a series of 'drip' campaigns, whereby messages are sequentially delivered for further reinforcement.

Communication timetable
continued.

• Stage 3: Validate

Week 5 +

Experts acknowledge that a greater chance of behavioural change occurs when training is validated.

This can be easily done by sending a validation piece to the employee. This piece asks the employee to comply, acknowledge and validate their understanding.

Validation is an essential step to ensure staff go beyond the mandatory paper compliance; it helps effect behavioural change and develop a strong security culture.

Good practice is to follow up security training with a short quiz to test employees' understanding of the topic. Outline a variety of security-related scenarios, with multiple choice answers. Use the results to identify those staff who require further training.

For deeper engagement, introduce gamification into the learning mix. This can be done either pre or post classroom training. Leader boards, time challenges, puzzle solving and other 'games' incorporate competitive elements that appeal to human nature. Challenges and rewards compel learners to make decisions, and so reinforces learning and retention.

Security topics

Here are some of the main themes to help create a security culture within an organization.

- **Online behaviour** – vigilance when using social media; secure email and online-browsing practices; payment card protection.
- **Computing conduct** – the importance of strong passwords and storage of passwords; reliable firewalls and anti-virus software; secure on-and-off-site data storage practices.
- **Insider threat** – accidental or wilful leaking of classified information.
- **On premise security** – swipe card/biometric access, visitor access, after- hours access.
- **Remote working** – secure practices while working out of the office; Wi-Fi networks; safeguarding digital devices and data; Bring-your-own-devices on company networks.
- **Social engineering** – protection against phishing, caller ID spoofing.
- **Asset security** – safeguarding company property.
- **Personal security** – care and awareness for personal security at all times.

COMMUNICATING TO THE INDIVIDUAL

Security-conscious behavior is the responsibility of each individual. Here are some pointers to get the right mix, format and content to suit different learning styles.

Make your message personal

The messages must be relatable to the employee. Focus on how they – and their family – can personally benefit from improved security awareness, especially at home. For example, an education campaign that's designed to make their loved ones safer on the Internet is likely to resonate more than focusing on protecting the organization.

Target by role

Some staff have privileged access to confidential documents, and require extra layers of security. Segment your staff into groups and customise their training to suit. Using SnapComms employee messaging software, you can easily target messages to specific groups based upon business need.

Cut-through the noise

Staff are bombarded with information these days, so finding a way for important security awareness communications to stand out from other 'noise' is vital. SnapComms visual messaging software is designed to do just that, ensuring important communications get noticed. Desktop alerts, screensavers, and wallpapers are just some of the channels that reliably get employees' attention.

Tracking progress

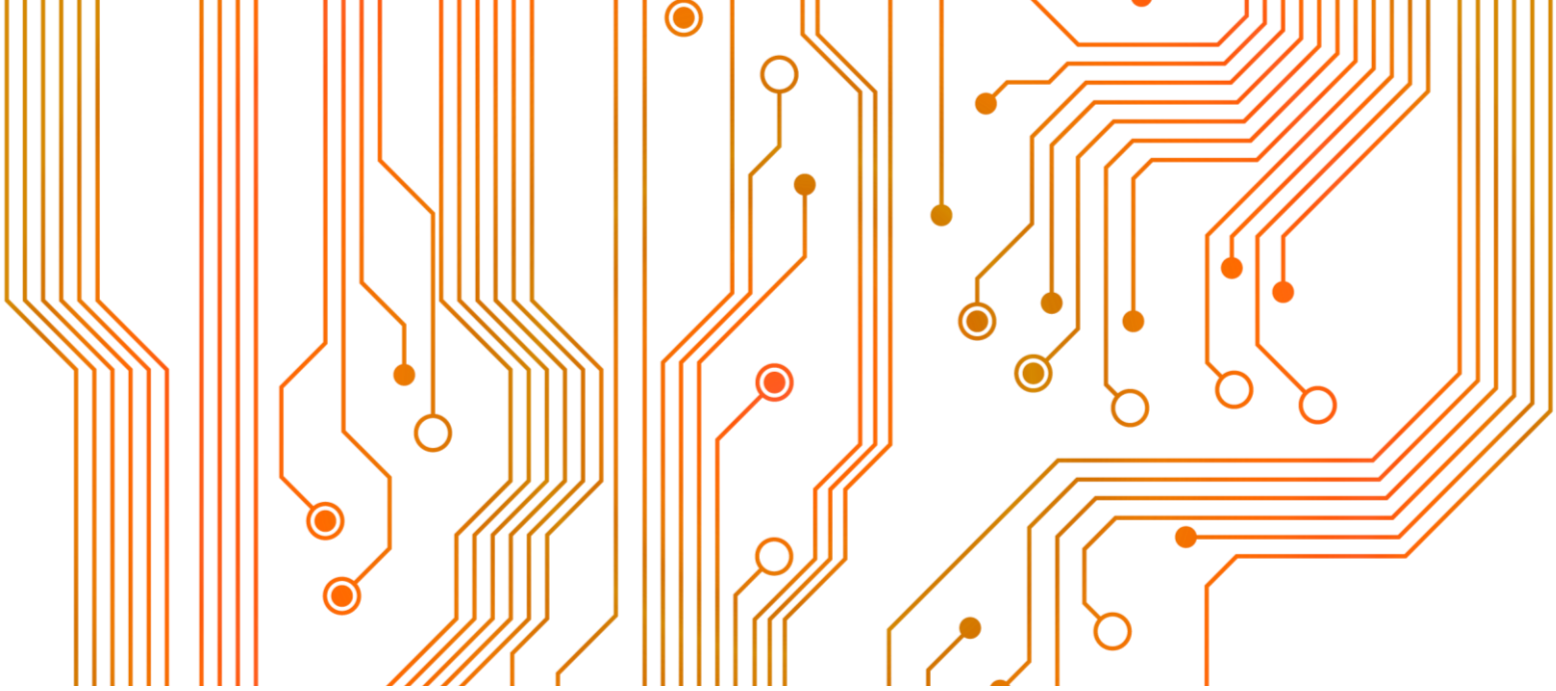
Monitoring the effect of a security awareness campaign reveals what's working and what's not. These days, this can easily be done by tracking delivery of messages and click-through behavior. Validation tools are essential as they identify those staff who have or have not completed and understood the training.

Keep messages simple x 3

People tend to remember things easier if they are listed in threes. Just think of 'Stop. Look. And Listen' as a case in point. Avoid using technical security language, and keep messages short.

Develop a theme

Identify a potential theme to help get your message across. 'Cars' for example, is a popular option for security campaigns as there are shared similarities i.e. safety, protection, locks. Remember, the more visual the better.



CONCLUSION

No person or company is immune from a security threat. Those most at risk are those with little or no security planning in place.

Developing a security culture is no longer a low priority for organizations: it's now a vital part of the fabric. Pro-security behaviour is being woven into systems, processes and the daily routines of employees.

Getting staff on board and changing their behaviour requires careful planning of internal communications. A well-constructed program which allows for messages to appear in sequence, using a variety of highly visual and engaging channels, in unmissable formats can help create maximum impact and message absorption. Most importantly, validation is a necessary step to ensure staff go beyond basic 'paper compliance'. Acknowledge that security awareness is an ongoing project that will only be as effective as the communication program underpinning it.

Are you ready to improve security awareness in your workplace?

Learn more about security communication

SnapComms

Get Employee Attention

SnapComms is a global leader in internal communications software, serving many of the world's largest organizations.
Formed in 2007 to address the issue of information overload in the corporate environment, SnapComms' products enable organizations to communicate more effectively with staff by delivering important company messages directly onto devices such as PCs, Macs, smartphones and tablets.
A key feature of the solution is it bypasses email and guarantees delivery of the message (with full tracking available) SnapComms' software includes:

- Interactive screensaver messages
- Computer wallpaper messages
- Scrolling newsfeed headlines with clickable message boxes
- Pop-up emergency notifications and urgent desktop alerts
- Pop-up quiz and survey tools
- Employee-generated magazines and newsletters

Options include employee and device targeting, unread message display recurrence and escalation options. Messages are measureable in terms of their delivery and readership. SnapComms has offices in the USA and UK, and is headquartered in New Zealand.

Arrange a demo

No obligation, find out how SnapComms could help your business today.

BOOK A DEMO NOW

Contact us

Every organization has a diverse internal communication needs. Contact us to discuss yours with our experts.

www.SnapComms.com/contact-us

Request a quote

For a personalized quote for your business, email us here.

info@SnapComms.com