

SIT PRESENTS



CYBER  
INFLUENCE  
GUIDEBOOK



# Table of Contents

This handbook and works within it are issued under Creative Commons, NonCommercial (CC BY-NC)



This license lets others remix, tweak, and build upon your work non-commercially, and although their new works must also acknowledge you and be non-commercial, they don't have to license their derivative works on the same terms.

A little note: we encourage organisations to use, share and distribute this guidebook to their customers and publish its contents freely, but they should not use it in explicit marketing, products, or services.

<https://creativecommons.org/share-your-work/licensing-types-examples/#by-nc>

Foreword

1



Influence vs  
Awareness

2-5

## Components of an Influence Program



Face-to-Face  
Training and  
Presentations

8-11



Writing for  
Influence

12-15



Events

16-19



Phishing Drills

20-23



Security  
Champions  
Programs

24-27



Videos

28-31



Collaboration

32-35



Metrics

36-39



# Foreword

ACSC

Rachel Noble PSM  
Head, Australian Cyber Security Centre

With nearly every one of us using a computer or mobile to communicate, to store data and interact with customers, cyber security has never been more important in the workplace. Our employees are one of our biggest assets and we need them to set the example and help protect both the corporate knowledge and the information that belongs to customers.

Large employers such as retailers and Australia's telecommunications and finance industries deliver cyber security awareness programs to their staff across the country and have learned much about what works to improve security culture in their workplaces. However, 89 per cent of Australian businesses are microbusinesses of less than five employees, and not all have the resources to develop cyber security awareness programs for their staff.

The Security Influence and Trust Group is made up of cyber security awareness professionals from businesses and institutions across Australia who are rethinking how we move from tick-the-box compliance training to genuine staff engagement on cyber security. In other words, how to go beyond awareness-raising to influencing the behaviours and actions of leaders and staff.

Cyber security incidents have been estimated to cost Australian businesses up to \$29 billion each year. Cybercrime poses a major risk to our community with over 13,500 reports of cybercrime being made to the Australian Cyber Security Centre since July 2019, at a rate of approximately one every ten minutes. Cybercriminals operate at scale, applying the principle of 'quantity over quality'. They target individuals and business by exploiting poor cyber-hygiene practices, including the use of default, simplistic or generic passwords.

Cyber security is a problem that needs a shared solution through collaboration between government and industry. The Security Influence and Trust Group are leaders in sharing experiences and programs to help organisations improve their safety cultures in the office and beyond.

This guide is a practical resource that will inspire organisations to build cyber safe cultures and empower staff. You will find insights into phishing simulations, security champions programs and creative ways to engage your staff in cyber safety.

I commend the authors and organisations who have produced this guide, for sharing their knowledge and expertise from fields as diverse as retail, telecommunications and finance.

Organisations, small or large, private or public, in any line of business, will benefit from their experience and make an important contribution to improving Australia's cyber security.



# *Influence vs Awareness*



People play a fundamental role in an organisation's cyber security defences. They, as part of a strong security culture, can act as a force multiplier.

However, the power of people as a security defence is realised only when security culture programs evolve beyond raising awareness to winning hearts and minds. This is the journey from awareness to influence.

## *The problem with awareness*

Traditional awareness programs are ineffective at best. Their failure to improve security culture leads some security practitioners to consider technical solutions superior to those that would improve the security savviness of staff.

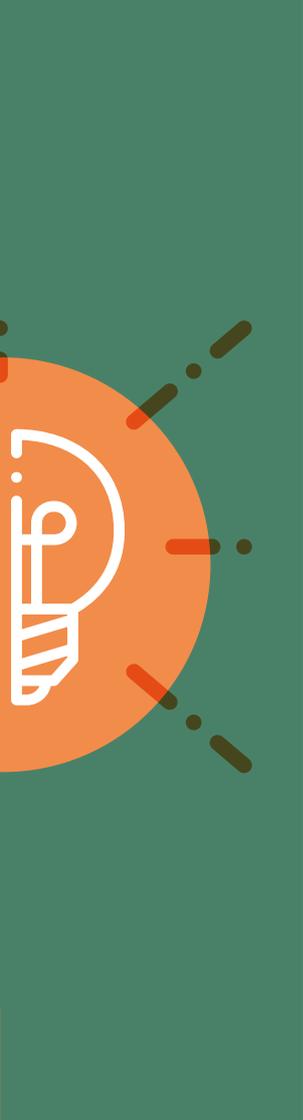
These programs will often:

- ◆ Force-feed information annually to busy staff, driving them to guess their way through multiple-choice questionnaires;
- ◆ Publish long, dry policy documents and advisories on an intranet site that remain unread;
- ◆ Lecture and threaten staff and ultimately discourage them from engaging with and caring about cyber security.

Awareness programs are usually a conduit for security teams to project their priorities on staff. The programs dictate to staff what security thinks they should know in often unwieldy and unpopular content formats.

It is more effective to facilitate the needs of staff by learning what drives their behaviour and what is the most effective way to engage them.





## *From awareness to influence*

Influence is the outcome awareness programs hope to achieve. But achieving it requires more than just an understanding of cyber security; it requires a thorough understanding of employee needs and motivations.

Staff also need information that is relevant and actionable and which can be easily and enthusiastically retained. It must ‘stick’ and be a motivating force for change.

## *A model for influence*

Despite being written over half a century ago, Harvard psychologist Herbert Kelman’s 1958 paper [\*Compliance, identification, and internalization: Three processes of attitude change\*](#) on social influence provides a model we can equally apply to influencing cyber security behaviours.

It examined the drivers for attaining attitude change that is “durable” in that it is lasting and extends beyond public conformity to private acceptance, where beliefs are integrated into an individual’s own value system.

These drivers can also be applied to influencing cyber security behaviours.

### *Compliance*

Change will occur when individuals look to gain reward or approval, or to avoid punishment or disapproval – this is the goalpost where most traditional awareness programs finish. However, while compliance may help drive acceptable behaviour, it will not necessarily translate into a change in belief or result in *lasting* change.



### *Identification*

People are more likely to be influenced by those with whom they identify; think brand and reputation. No matter how good your advice may be, if you haven't established credibility or trust with your audience, your ability to influence will be diminished.

As influence practitioners we must therefore establish credibility or trust with our audience and reflect on how the security team is perceived – as a blocker, or as a trusted partner?

### *Internalisation*

Lasting change is ultimately achieved when people have internalised the message and taken on our beliefs as their own. They are no longer doing something because they've been told to, but because they believe it is the right thing to do and is in their interests to do so – the new behaviour is intrinsically rewarding.

## *Human problems require human solutions*

Security education therefore needs to be more than simply providing information to people; it must be targeted, actionable, and achievable, with simple consistent rules of behaviour that people can follow.

It must be relevant to their roles and interests, free of jargon, and composed of plain language, case studies, metaphors and allegories to explain the why (not just the what), provide context, and build a conceptual understanding for the audience.

Advice must ultimately motivate the audience to take an action because it is in *their* interest to do so — not yours.

It is not just *what* you say, it's *how* you say it. Lasting change requires advice that is understandable, relatable, and engaging.

Security culture change takes time but, with the right expertise and focus, it can lay the groundwork to ultimately weaponise what is simultaneously the biggest strength and weakness in most companies' cyber security posture: their people.

This guide shares insights and examples from cyber influence professionals to demonstrate how this model is being practically applied to evolve traditional awareness activities into programs tailored towards influencing behaviours and decision-making.

# INFLUENCE



□ *Components of  
an Influence  
Program*



### What?

In-person staff presentations.

### Why?

It is one of the most effective ways to engage with your audiences and is immediately available to new influence programs.

**Resources:** *The Tipping Point*, *Made to Stick*.

**Begin:** Consult the SIT website for a list of good topics to discuss. Reach out to existing staff networks or friendly teams to build attendance.

# Face-to-Face Training and Presentations



It felt like I was back at school during one of those afternoons that seemed to drag on forever. I could even hear the clock on the wall, optimistically ticking through the silence after I asked the training group if they had any questions.

Their glazed-over eyes, their mindless doodling, and the few in the back trying to discretely answer emails on their phones - politely flicking their eyes up on the odd occasion while nodding enthusiastically at the wrong times; it seemed my immaculately planned presentation on security awareness was falling flat.

I learned the following lessons the hard way.



## Lesson

# 1

## Meet your audience where they are

Be mindful that staff have their own priorities and workloads to juggle, on top of your training. If the group you are presenting to has a weekly stand-up, monthly ‘town hall’, or quarterly ‘all-hands’, consider booking a spot during the meeting rather than organising a stand-alone session.

The team will appreciate something different on the agenda, while you will reduce the time spent on admin by not needing to book meeting rooms or wrangle attendees, and can be confident you won’t be presenting to an empty room. If joining an existing session is not possible, consider a ‘lunch and learn’ or brown bag session.



This works especially well for non-compulsory training sessions and can all but guarantee attendance if you throw in some free donuts (*donut* just take my word for this!).

After your presentation, find out how to integrate your messaging into reoccurring meetings throughout the year to reinforce your key takeaways. Your agenda items will be better received if they are similar to a team’s existing items; many teams open meetings with ‘safety issues’ so starting yours with ‘safety and security issues’ is a good idea.

## Lesson

# 2

## Work out what your audience truly cares about



SIT’s Craig Templeton often says, “there’s no interest like self-interest”. This speaks to how advice about security in the home trumps tired traditional office-based security guidance and helps to put security in the front of mind of staff. Improved security hygiene at home will eventually translate into secure behaviours at work.

Nothing makes your audience pay more attention than the question of “*what’s in it for me?*” To help with profiling each group or segment, you might conduct a ‘voice of the customer’ survey. This could be as simple as grabbing a clipboard and interviewing employees during their morning wait for the elevator or sending an email in advance of the training with a “*help me to help you*” vibe.

What makes your audience tick? What security issues are relevant to their department or job responsibilities? And why should they care about what you have to say?

Use the knowledge you gain into your audience to create content that connects with their needs and (self) interests.

## Lesson

# 3

## *Make your message stick*



We all remember the story; a man visits a bar in a new city and is approached by a woman. She buys him a drink, and that is the last thing he remembers until waking in a bathtub full of ice – sans kidneys.

Why do we remember this story, yet have trouble recalling the last few security presentations that we attended? It is because nothing sticks better than a good story. Malcom Gladwell explains the concept of 'stickiness' in his book *The Tipping Point*: some ideas stick in the mind, while others do not.

Read widely for analogies ([theanalogiesproject.org](http://theanalogiesproject.org) can help) or recall the firsthand experiences of your (anonymised) friends and family.

Jump on nearby bandwagons; if your staff are binging on the latest Netflix release, then leverage the cultural hype where possible. Can you develop a meme, analogy, or parody based on the storyline?

What about current events? Has there been a topical data breach of late?

For a super sticky message jump on [www.hibp.com](http://www.hibp.com) and demonstrate live whether a volunteer in the room has a compromised account connected to their email address.

“there’s no interest like  
self-interest”.





**What?**

Effective writing is a skill that requires study and practice, not just literacy.

**Why?**

Great writing wins readers and is a keystone of cyber security influence. It sells ideas.

**Resources:** Non-default Word spellcheck options. Grammarly. Various courses.

**Begin:** *Made to Stick, Grammar and Me, Eats Shoots and Leaves, On Writing, SIT's writing guide.*

My favourite keys on my laptop are in a sorry state: the broken left arrow lists like a crippled ship, the right is stuck fast, and the down arrow is completely gone, leaving white backlight gleaming in its place.

Only 'D' and 'te' remain on the delete key. This wreckage is a tribute to how often those keys have whittled my verbose self-indulgent writing to poignant clarity.

Delete is a painful key to master but it is also a writer's most valuable. It whittles treasured but excessive ideas and loved but confused poetic prose. It leaves behind the cyber security influence practitioner's goal of simple, effective writing.

## *Writing for Influence*



## Audience

Good writing is written for a defined audience. A newspaper sold to anyone on the street is still written for a particular reader of a particular age, gender, political persuasion, and socioeconomic status. Trade publications, scientific journals, and radical university newsletters more obviously serve a target readership.

Writing for Telstra's staff is like writing for a national newspaper. My readers are developers, call centre operators, retail shop staff, suited executives, and field staff in hi-vis vests.

They are simultaneously competent and unfamiliar with technology, concerned about their kids' online lives and child-free, interested in hacking and bored by it.

Each piece of writing must be written with one or more of your audiences front of mind.

## Message

Your writing must be written *for* your reader, not *at* them. It should be relatable, entertaining, and helpful, not abstract or dictatorial. Speak to your readers as regular people, not staff. Your security message should be seated in the context of your readers' values, or even subservient to them.

Use concrete, plain language terms. Do not adopt your corporate marketing teams' invented words, capitalisations, and focus-group slogans. Broadly speaking, if it doesn't exist in a Macquarie dictionary, it doesn't exist (*common* technology terms exempt).

Realise [the more you know about a subject the worse you are at explaining it](#). I find reading your story aloud helps. Bend the ear of an honest colleague and read them your opening two or three paragraphs. Don't explain the story to them beforehand as they need to understand your message as an outsider.

If you are on your own, read your story aloud to an imaginary stranger. You should find yourself reducing your sentences to simple English.





## *Structure*

The opening sentence, or lede, sets the mental trajectory for my writing and I spend most of my time rewriting it.

For me it is akin to lining up a 10-pin bowling shot. You may not be the same, but you should have a good idea of where your writing is heading, and how each paragraph helps build the story.

Journalists invented the inverted pyramid of writing 150 years ago as a means to ensure the most important facts were sent first from war theatres' news bureaus. The story had to get out over failing communications lines.

They follow it for hard news today. You should too.

## *Read*

Good writing isn't easy. It doesn't come with language fluency. It comes like anything worth doing from practice.

Stephen King said to be a writer you must above all else read a lot and write a lot: "There's no way around these two things that I'm aware of, no shortcut".

Read broadsheet newspapers. Read trash mags. Read your favourite sugar-fix fiction. Study the narrative flows and see what style grabs you. Then write, write, write, until you, like me, need a new keyboard.

## QUICK TIPS

- \* Follow journalism's inverted pyramid.
- \* Adopt a style guide from an established media outlet. I recommend the BBC's.
- \* Define your reader and why they should care about your idea before you write.
- \* Not all influence writing needs a lesson. Writing for entertainment is a gift to readers.

**“YOUR WRITING MUST BE WRITTEN FOR YOUR READER**

**...NOT AT THEM”**

## Events

My suspicion that events were an effective way to promote positive cyber security culture was confirmed when thousands of our team members poured through our stands during our Stay Smart Online Week event.

It was October 2018 and the Federal Government's flagship cyber security awareness event was in full swing, with many major corporations creating and broadcasting their own online safety campaigns.

My team had set up four stands in the central lobby at Woolworths' NSW headquarters to reflect four key pillars of cyber security awareness. It was a high-traffic spot; each office wing fed into the lobby through three arterial corridors.

Such high visibility meant that we would succeed or fail in front of everyone. There were 6,000 people in the office that day and it was my team's first cyber security event. We had to ace it!

### What?

Cyber security awareness events.

### Why?

Engaging staff in entertaining and informative events is an effective way to boost awareness and establish a friendly team reputation.

**Resources:** Inexpensive prizes, vendor-supported large prizes. Hacking demos, password strength checks, device health checks.

**Begin:** YouTube, HaveIBeenPwned, vendors you have relationships with.



STAY  
SMART  
ONLINE

A big reason for our success on the day was that we engaged our team members as regular people, not just employees. Our security advice addressed the needs and wants of team members both at work and at home in what we internally refer to as engaging team members at the 'home level'.

The home level was key to not only the event's success but in our efforts from previous years in recasting the image of our cyber security team as friendly and helpful, moving away from old perceptions of the team as a blocker and disciplinarian.

Our event was also designed to be fun. Team members played games and competed for prizes, donated and awarded by Woolworths technology partners. Team members who asked questions of each stand had a passport stamped which entered them into a draw for a major prize.

### *At home*

Our 'at home' stand focused on passwords and showcased the importance of strong and different passwords across accounts. Our cyber security team members gave practical and accessible answers to questions from our team members.

This stand's game was to create a strong passphrase. Team members created a strong passphrase then typed it in again to eliminate the possibility they selected one at random.

Once entered, the passphrase would be rated as 'weak', 'satisfactory', or 'strong' depending on the length, characters used and any associated letters or numbers. Team members that could create and verify a strong passphrase received a small giveaway prize.

### *At work*

A spinning prize wheel was the centre of our cyber security at work stand. Team members were refreshed on Woolworths' cyber security policies by answering real-world questions relating to the handling of sensitive information, data classifications, and broad questions relating to cyber security and our team.

Team members spun the wheel and answered a question associated with each icon. Small prizes were handed out for correct answers.



## *Out and about*

Phishing and scams were as always of huge interest among our team members and customers. At this stand, we warned of the rise of SMS-based phishing and gave examples of the phishing attacks we see in Woolworths' hoax reporting inbox (where employees are encouraged to send suspicious emails).

We also gave out prizes as part of a pin-the-tail on the scam game. Again, we rewarded correct answers with a small prize.

## *Office of the eSafety Commissioner*

The Federal Government held our final stand handing out information on how to stay safe online, how to report scams, and offering prizes to winners of a ball pong game.



## *Playing the long game*

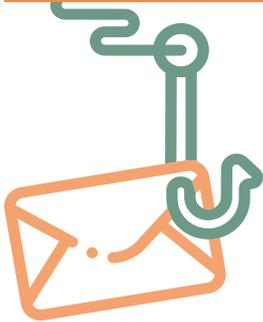


Events are a great way to engage team members on good cyber security behaviour and are an effective means to uplift and promote the Cyber Security team across the business.

Gamification is a highly effective education tool and means to promote cyber security discussions across the organisation. Rewarding positive behaviours with prizes, even small ones, will sell your security message.



“Rewarding positive behaviours with prizes, even small ones, will sell your security message.”



## Phishing Drills

My first proposal to management to commence phishing simulations *against our people* in early 2013 was a flop; our human resources team were rightly concerned.

They feared our phishing exercises may scare or pester employees, or worse, punish employees who failed the ‘tests’.

Many influence practitioners including my colleagues in SIT faced initial resistance from their business leaders when they pitched phishing exercises as an important function of cyber security. You may too.



### What?

Phishing drills – the next evolution of emergency preparedness – allow employees to experience phishing attacks in a safe environment.

### Why?

Phishing remains one of the most common and reliable cyberattacks. Drills help employees to develop the necessary skills to better recognise and report phishing attempts. Critically, they also open the door to broader conversations about cyber security.

**Resources:** Open source, free and enterprise solutions exist in a busy market.

**Begin:** PhishMe free, Gophish, Infosec IQ free

### Reel ‘em in

There is no silver bullet for bringing detractors on side, but reframing drills as an opportunity to improve resilience is one popular approach which may help.

Pitch phishing exercises to business leaders in terms they understand. Our human resources team pushed back on the idea of ‘testing employees’ but warmed a mere six months later to the concept when it was recast as the next evolution of emergency preparedness and dubbed ‘phishing drills’.

Just as we prepare employees for physical emergencies, so too we must prepare them for cyber incidents.

Consider automating feedback to staff who report phishing emails. A successful phishing program dramatically increases the rate of staff reporting suspicious emails, but this is only sustained if people can see the value of doing so.

This means providing staff feedback that demonstrates if their report was legitimate email, a phishing drill, or a nasty email that could've taken down the organisation without their swift action. Luckily some providers can help with platforms that send dynamic feedback for different reports.

Hit the right frequency of drills to minimise disruption, while ensuring phishing is front of mind. ANZ and other SIT organisations run quarterly drills which are considered the minimum interval to maintain efficacy of training.

Targeted drills for those audiences at greater risk or in need of tailored scenarios have also proven invaluable for building the skills to recognise and report suspicious emails.

An IVR phone message describing the current drill could also help minimise phone calls to already busy security operations centres.



## *Catch and release*

Employee interaction with phishing drills should be a fast and positive experience.

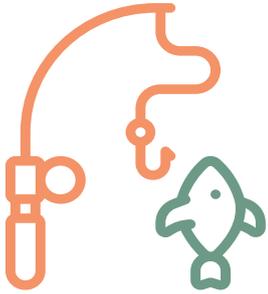
My SIT peers and I find real-time feedback for those who correctly report or fail drills is key to achieving this.

Reward your employees with a short sentence or two informing them that they have reported or interacted with a safe phishing drill email, what this means for the security of the business, and what to do next. Do the same for those who report real phishing emails.

Brevity is key as I have found employees spend an average of 10 seconds reading failure education pages before moving on. I recommend against embedding videos since audio can highlight an employee's drill failure to others in an office environment.

Employees must never be punished nor identified for failing a drill. We want our people to feel safe reporting their mistakes so that swift corrective action can take place.

Some organisations opt to enter repeat clickers into additional training or extra drills, but an avoidance of punitive action is established best practice – don't punish humans for being human.



## *Bycatch*

It can be difficult to predict the impact of some drills. Those based on a fake mail delivery can prompt staff to ignore links and instead call or visit mailrooms. Drills that use real brand names have leaked into the public arena causing embarrassment for organisations.

Drills can be disruptive. Thorough planning and broad stakeholder consultation help mitigate negative fallout from drills, however, you should accept that some employee reactions will be unpredictable. SIT members have seen employees call councils and government agencies in response to drills that directly reference neither.

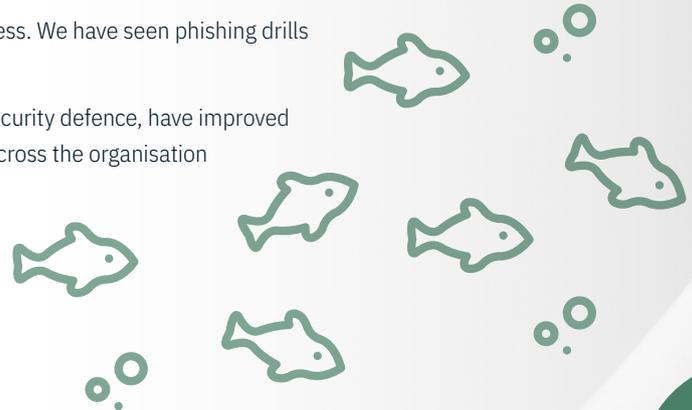
---

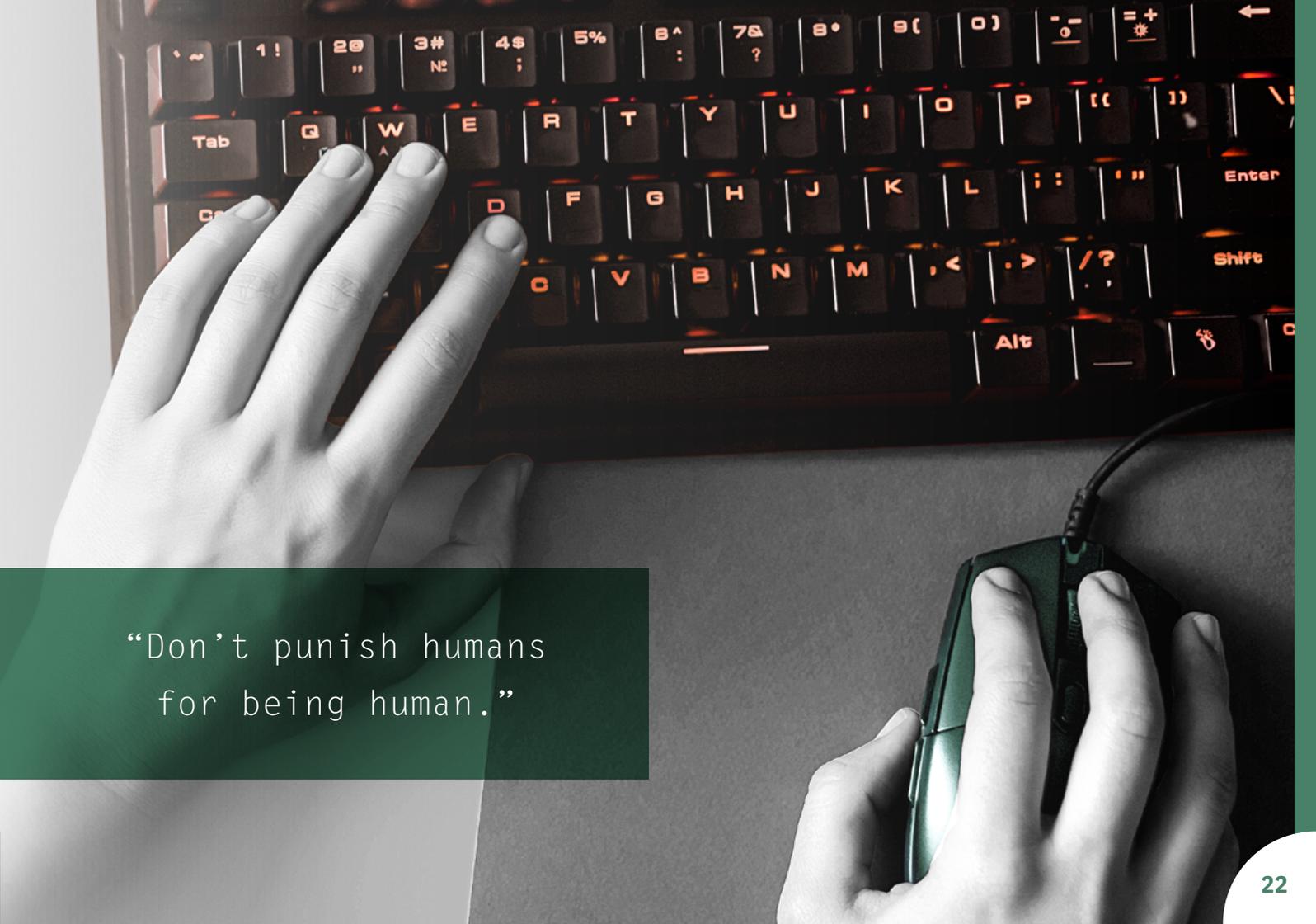
## *Sustainable phishing*

A well-designed drill will lead to wider acceptance by employees and the business. We have seen phishing drills become part of ANZ's corporate culture since their introduction six years ago.

Drills have reinforced our message that our people are critical to ANZ's cyber security defence, have improved the quality of real phishing reports, and importantly encouraged conversation across the organisation about broader cyber security challenges from frontline employees to executives.

Success for an influence practitioner is measured in part by cyber security becoming part of the vernacular of the organisation – phishing drills help to achieve this. A spot of friendly competition goes a long way.





“Don’t punish humans  
for being human.”

# Security Champions Programs

Lee Beyer  
QBE Insurance



## What?

A network of security advocates who amplify security messaging.

## Why?

Champions networks maximise and extend limited resources. They give otherwise unattainable levels of trust to messages. They provide unvarnished insight into company mindset and operations and serve as a light extended security team.

**Resources:** Find potential champions in company social media, staff directories, and by leaning on existing contacts across the business.

**Begin:** Social media posts, team meetings.

My first post in cyber security culture change was tough; it was 2011 and I was flying solo, charged with selling security to thousands of employees at a time when few people outside of the industry knew or cared about it.

Our corporate communications people had other priorities, which meant I found myself unable to broadcast over the centralised intranet homepage.

And so I set to work building my own communications network. What began as a handful of staff loosely interested in cyber security and scattered across the organisation's diverse units became a tour de force of more than 300 champions bringing positive security culture into every area of the organisation.

Such was the force multiplier success of the champions network that I believe it should be a centrepiece of security awareness and influence for the largest global enterprises down to medium businesses with a hundred staff.

## Cons

- ◆ Need to maintain good content and events to keep champions engaged
- ◆ Administrative maintenance of memberships
- ◆ Enthusiastic champions may give erroneous security advice



## Pros

- ◇ Extend your security team's detection and prevention capabilities
- ◇ Build trust by providing employees with a 'look under the hood'
- ◇ Gain significant loyal engagement
- ◇ Forge new highly effective communications channels
- ◇ Bypass corporate communications blockers
- ◇ Increase receptiveness to your messages by leveraging the influencing power of your champions within their own networks
- ◇ Gain insight through feedback into the cyber security priorities or frustrations of different teams



## *Getting started*

Consider your champions network akin to an occupational health and safety (OHS) network and set it up with an aim to have a representative in every unit in your organisation. These champions will be the go-to people for cyber security issues in their units.

Establish how many champions you can handle. You will be able to handle more champions if you plan repeatable and scalable initiatives like newsletters, articles, and presentations from your security team. Consider how you might automate the champion enrolment and unsubscribe process.

Then start small and let your engaged network grow organically over time.



## *Building out*

Once your first champions have joined and are engaged, begin to promote your program as much as you can. Open your network to everyone and disregard seniority:

- ◆ Include reminders in online and face-to-face training (e.g.: “if you liked this content, then consider becoming a champion”)
- ◆ Offer it to proactive people who report phishing or suspicious matters, or who show curiosity (e.g.: “great job reporting this email, Darren, it was a phishing attempt. We think you’re pretty savvy and would welcome you to join our champions network”)
- ◆ Include a call to action at the end of intranet articles

## *Reward and recognition*



Your champions are special, so treat them that way.

- ◆ Offer them a first look at security or technology changes being deployed (pilot groups)
- ◆ Ask their opinion on new initiatives
- ◆ Give them early insight into phishing tests and results
- ◆ Provide them with deep dives on breaches, attacks, and staying safe online
- ◆ Invite them to security events
- ◆ Make your champions recognisable with a special badge or lanyard
- ◆ Give them if possible cool, appealing security-branded merchandise like webcam covers and monitor privacy covers
- ◆ Have the head of security name them as extended members of the security team which is useful for their personal performance conversations

### *What's in for them?*

- ◇ Development opportunities (stretch KPIs)
- ◇ Recruitment pathways
- ◇ A chance at a new and unexpected career (and you get skills you didn't know you needed)



“Your champions are special...  
so treat them that way.”



### What?

Cyber security awareness videos.

### Why?

Engage with audiences on popular modern platforms.

**Resources:** Lightworks (free), Shotcut (free), OpenCut (free).

**Begin:** Free videos: *Data to Go*, *Dave the Psychic*, *Companies like You*.

## Videos

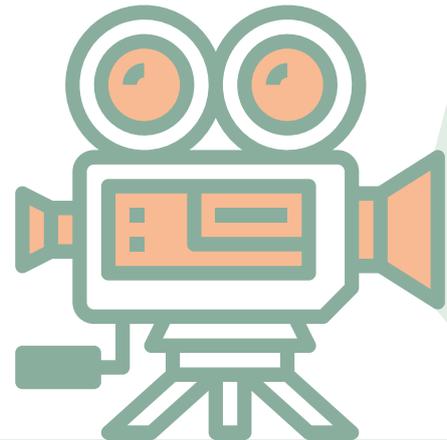
“The thing you’re doing now, reading prose on a screen, is going out of fashion,” the *New York Times* wrote in a 2018 obituary to the written word titled *Welcome to the post-text future*. It claimed videos, along with photos and graphics, are dominating our online experience.

Consuming information through text has lost popularity among younger audiences in an age of podcasts, YouTube, Snapchat, and Instagram stories, but it is far from dead. Everyone consumes information differently and there is still an audience who continue to prefer a good read over watching a video.

As a cyber security influence practitioner, you should likewise consider your readership. Chances are they are similar. Video, therefore, should be a core medium of your influence program.

It is not just about catering to an audience’s taste: neuro-imagery shows that consumers primarily use emotions rather than information when evaluating brands. It also shows that events that trigger emotions and subsequent dopamine release significantly increase the ability for audiences to recall information.

I have found that using positive emotion-provoking genres, such as comedy, is a great way to imprint your message on consumers.



## *Mediums and methods*

I have worked with creative agencies and studios to produce over seven videos – from short educational animation to big production live action – to educate staff on how to identify and avoid cyber security threats.

I worked in concert with incident response, assurance and risk management teams to discover and select the most relevant topics and advice. I also co-ordinated closely with executives, HR and internal communications to understand priorities and set an appropriate tone.

The live action videos told of the need for password management and information protection, and of threats such as social engineering. They were a hit, especially with our younger staff viewers.

## *Before you start*

Take the time to think about your message (**the what**), explain its importance (**the why**), and provide staff with a takeaway action (**the what next**). Workshopping with colleagues really helps to flesh out your ideas and next steps.

## *Map out your stakeholders*

Engage your stakeholders right from the start as they may have huge bearing on its development and success. This will especially help you avoid the need to rework videos at a point where doing so is difficult and expensive and could blow budgets and deadlines.

Get them involved early and earnestly. Some stakeholders to consider engaging:

- ◆ CISO/CSO
- ◆ HR (particularly if your content is a bit edgy)
- ◆ Corporate communications
- ◆ Marketing and brand

## *Create a timeline*

Write and clearly communicate to your stakeholders a timeline with milestones (including all draft and final versions of scripts and storyboards). Give yourself time buffers.

## *Length*

Audience attention spans dictate that your videos should be no longer than about two minutes and 30 seconds, though I recommend even shorter for a maximum of one minute and 30 seconds.

Rules can be broken in rare instances. SIT members working with a professional creative agency have produced videos four minutes in duration which still achieved audience retention rates in the 90th percentile thanks to a strong and engaging narrative.

Such efforts are gambles, though, and you are strongly advised to keep videos short and edit heavily during your first cut.



## *Development*

The culture of your organisation will shape the tone, length, and format of your videos. You may wish to borrow themes and styling from established popular television series and platforms where appropriate.

## *The power of sound*

There are many royalty free and cheap music tracks to greatly enhance your video's narrative. Research what sounds work best for your video's themes and what is appropriate for your organisation.

Buy a set of good stereo speakers.





## *Diversity and inclusion*

Seriously consider the names, genders, ages, and ethnicities of your characters. A good rule of thumb is to mirror your workforce's cultural make-up.

## *Accessibility*

Keep the language of your video simple for the benefit of viewers whose second language is English and use closed captions. Subtitles also help if you display your videos on screens in areas such as lobbies.



## *Review cycle*

Send your stakeholders the scripts and narratives for your video for consideration before pulling everyone into one room for a single rigorous review. Avoid as much as possible having multiple documents from different stakeholders as conflict resolution will be difficult.

Get your stakeholders committed with their agreed workshop changes and avoid allowing continuous review. It will become expensive and challenging to change things later.

“Consumers primarily use emotions when evaluating brands.”



Laura Hartley

NAB



**What?**

Cyber security influence collaboration initiatives between organisations and government.

**Why?**

Collaboration amplifies important key messages, grants access to content resources, and paves the way for future opportunities.

**Resources:** the [Office of the eSafety Commissioner](#), the Australian Competition & Consumer Commission's (ACCC) [Scamwatch](#), the Australian Cyber Security Centre's (ACSC) [Stay Smart Online](#), [Office of the Australian Information Commissioner \(OAIC\)](#). Financial organisations including banks also provide helpful resources on spotting scams, as do agencies like the Australian Tax Office.

**Begin:** Join the SIT Group.

# Collaboration

Cyber security is often said to be a team sport. Effective cyber defence is a joint effort between security professionals and computer users – but it also speaks to the need for organisations and government to work together to increase cyber security awareness among the public.

Collaboration between organisations and government serves to amplify cyber security awareness efforts among the general public. This, ultimately, will lead to organisations hiring and engaging better informed staff, partners and vendors, and benefiting from a customer base who are better able to detect and avoid scams.

Cyber security influence practitioners can learn from industry and government, and gain access to resources such as guides, posters, case studies and videos to help consumers and businesses better understand and respond to cyber security threats.

Working alongside industry peers and aligning messaging can boost the effectiveness of campaigns and events, while sharing insights can improve the likelihood of behaviour change.

Collaboration also provides exposure to potential opportunities across industry, government, and academia and provides a platform for security influence thought leadership. For NAB, collaboration with industry and government has helped advance fraud messaging for both employees and customers.

NAB builds campaigns and events for employees, customers, and industry peers working closely with groups such as the ACSC in its Stay Smart Online initiative, the ACCC for Scamwatch's Scams Awareness Week, the Office of the eSafety Commissioner for Safer Internet Day, not-for-profit IDCARE, and the SIT Group among others.

Being a partner in a government initiative demonstrates your organisation's commitment to online safety and security. You're able to leverage the content and resources to develop security information that is timely and relevant, and to support annual campaigns within your own business.

While cross-organisation and government collaboration can be key to increasing awareness, without a clear strategy it can meander into group discussions without discernible or tangible outcomes. To ensure your collaboration is meaningful and achieves the outcomes you or the collective group require, here are some ideas on how to keep things on track:

- ◆ Know what the problem is that you are looking to solve – write it down, workshop it until you are clear on what the problem is.
- ◆ Consider what advice or expertise you need: if it's a small local problem, then a small local group might be sufficient, but if it's a larger issue consider broader engagement.
- ◆ Get buy-in before sending the invitations, and be clear on what will be discussed. There is nothing worse than being invited to a meeting that you didn't need to attend, or have nothing to contribute, so confirming you have the right contacts is critical.
- ◆ What lead time will you need? A national campaign will take far longer than you expect, so ensure that you have enough time to achieve the outcomes you're after. Also, different organisations have different policies and protocols. Something you might be able to deliver quickly could take longer for others. Ask for materials and start internal stakeholder engagement early to avoid delays.
- ◆ Always have a chairperson and a scribe at the meetings, so ensure that actions – the most important part of the meeting – are clearly captured.
- ◆ Make sure you call out, recognise, and thank people as you are progressing, and at the end of any joint initiative.

There are, depending on the level of involvement, opportunities to co-produce content, work on government projects, and benefit from cross-promotion for events and activities.

NAB has also worked with the Australian Computing Academy at the University of Sydney, ANZ, CBA, Westpac, and British Telecom to create a series of Schools Cyber Security Challenges. This cross-industry and academia collaboration has been a great initiative to address the cyber security skills shortage, and work alongside industry security leaders, education leaders, and curriculum experts.



- ◇ Access to up-to-date and trusted security information and resources
- ◇ Provision of consistent security messaging across businesses to increase exposure
- ◇ Access to education resources to share with your audiences
- ◇ Builds your corporate social responsibility and reputation
- ◇ Increases your brand recognition as a safe business



## Key calendar events

	Privacy Awareness Week <i>May</i>	Safer Internet Day <i>February</i>		
		Tax time <i>June</i>		Scam Awareness Week <i>August</i>
		Stay Smart Online Week <i>October</i>	SIT Summit <i>November</i>	Christmas <i>December</i>



“Cyber security  
is a  
team sport.”

## Metrics



It is difficult to gain insight into the efficacy of cyber security influence programs because raw

metrics lack context and true meaning. This is known as the causation-correlation conundrum.

However, I have hope. Metrics such as those available for the seven elements of an influence program detailed in the previous pages are useful as indicators of influence work and should be combined with other data points to paint a picture of wider behaviour and culture change.



### What?

How do you measure the impact of cyber security influence?

### Why?

We need to know the efficacy of cyber security influence programs and their effect on organisational security culture change and if it made a difference.

**Resources:** SANS security awareness roadmap, SANS security awareness maturity model.

**Begin:** Capture article hits, event attendance, phishing drill statistics.

### *The quicksand of reason*

Influence practitioners should be mindful of vanity metrics when measuring their influence programs. Metrics can often show large but vaguely meaningless numbers that may give a false indication of success. I call these busy metrics: interesting but not actionable in a meaningful way.

Vanity metrics purely help the influence practitioner understand if their engagement approach is effective. Ultimately, however, success for our profession hinges on sustainable behaviour change. This is much harder to measure, but much more important.

Give vanity metrics, such as article hit numbers, less weight than actionable metrics, like story comments and shares on social media. Ask yourself if actions you are measuring are truly responsible for behaviour change, or if a secondary factor is more likely the cause.

## People as 'vulnerabilities'

Whether you are following a pathway of security compliance or cultural change will dictate if you see people as vulnerabilities or strengths (see *Influence vs Awareness* page 2).

Compliance metrics provide a baseline important to understanding the effectiveness of an organisation's controls and risk appetite. They are binary, predictable, and can be benchmarked with external sources.

But compliance does not equate to security; it is likely most companies breached over the last 10 years were compliant with many security standards.

These metrics are therefore table stakes, and you need to evolve from them if you want to show that you see people as a control and your organisation's greatest strength, and not as vulnerabilities.



## People as 'controls'

Put simply, compliance metrics measure what people do when someone is watching. People comply with many things they don't truly believe in.

Behavioural metrics, on the other hand, measure what people do when no-one is watching. It is the things we do and discuss in private that we truly believe in.

These superior behaviour metrics measure people as a variable security control. Organisations which measure these metrics view staff as their greatest potential strength whose varying effectiveness can be improved over time.

My favourite metrics are the instances of influence that occur between peers such as when a friend tells another about how to spot a phishing attempt. That's winning and viral education, at scale. It relieves the cyber security influence team of the role as sole educator of threats and mitigation strategies.





However, it is difficult to measure these peer-to-peer learning moments as a quantitative metric. Instead, I capture any of these I encounter as qualitative metrics.

An example is how we capture our phishing metrics at REA Group. Sure, we could measure click rates, but what's more interesting is how many staff inform their colleagues about phishing risks within our dedicated Slack channel.

About 200 active users, or about a quarter of our Australian staff, have subscribed to that channel where they continually discuss suspicious emails and new phishing techniques.

This is 100 percent attitude and positive behaviour, with a low barrier of entry. It is significantly more valuable than compliance metrics.

## *More metrics*

### Compliance orientated:

Hits or checkbox numbers for policy, advisory, and training completion.

### Social media:

Discussion of cyber security, sharing of cyber security content.

### Articles:

Hits, subscribers and newsletter sign-ups, shares, comments.

### Champions network:

Number of enrolled staff, spread of staff across business units, engagement in program events and content such as articles.

### Incidents:

The number of security incidents reported by staff.

### Time to patch:

Mean time to patch and time to deploy.

### Sentiment polls:

Staff inclination to take steps to secure personal and company data.

### Targeted events:

Attendance to events such as brown bags are a useful vanity metric that should be ideally coupled with data from surveys or quizzes that evaluate attendees' information retention.



## *Playing the long game*

Metrics are part of an overall measure of the maturity of an organisation's cyber security culture. Smaller organisations can improve a negative or apathetic security culture faster than can global enterprises, but influence practitioners at both should be prepared to play a long game.

Those with new or burgeoning cyber security influence programs should begin with easy-to-measure metrics and work to balance or replace vanity metrics with those that measure actual behaviour change and show which efforts lead to the most improvements in culture.

The cliché of “you are what you measure” rings true; if you measure compliance, that's what you'll get, but will you be safe? If you measure culture, are you compliant?

Choose the balance that's right for your business. Start small, and grow.

“Behavioural metrics measure what people do when no-one is watching.”



# SECURITY INFLUENCE AND TRUST



Founded in late 2015, the Security Influence and Trust Group is a community of industry professionals who believe that collaboration, consistent messages and simple actions are key to empower people to protect themselves in the digital world.

The group provides an opportunity to share real-world experiences and strategies, so membership is restricted. However, if all or a significant part of your day job is dedicated to building security aware cultures, we encourage you to request to join the group via our LinkedIn page. We look forward to welcoming you into the community.



SIT 2019