GUIDANCE

10 Steps to Cyber Security

Guidance on how organisations can protect themselves in cyberspace.

IN THIS GUIDANCE

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

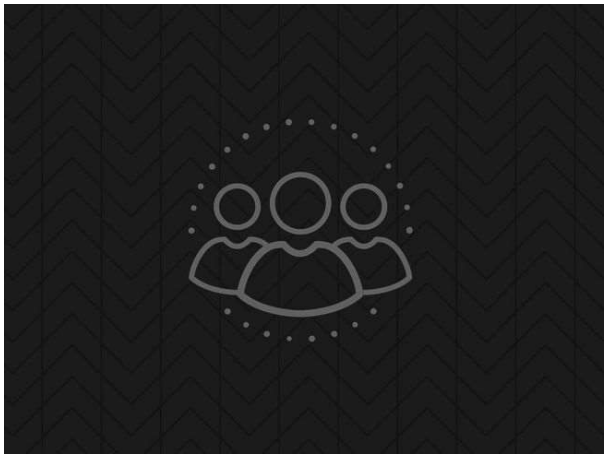
VERSION

1.0

WRITTEN FOR

Cyber security professionals

Engagement and training



Collaboratively build security that works for people in your organisation.

People should be at the heart of any cyber security strategy. Good security takes into account the way people work in practice, and doesn't get in the way of people getting their jobs done. People can also be one of your most effective resources in preventing incidents (or detecting when one has occurred), provided they

detecting when one has occurred), provided they are properly engaged and there is a positive cyber security culture which encourages them to speak up. Supporting your staff to obtain the skills and knowledge required to work securely is often done through the means of awareness or training. This not only helps protect your organisation, but also demonstrates that you value your staff, and recognise their importance to the business.

What are the benefits?

- **increased trust and loyalty to your organisation**
- **earlier detection of those incidents that are often not picked up by technology**
- **an environment where individuals feel safe (and are encouraged to raise problems and voice new ideas early) will make your organisation more effective**

What should you do?

Encourage senior leaders to lead by example

- Encourage senior leaders to set the tone when it comes to cyber security. If senior leaders ignore security policies and processes, or ask for 'special treatment' in some way (such as requesting a different device to those issued as standard), it sends a signal to everyone else in the organisation that seniors don't consider the rules fit for purpose, and that it's acceptable for staff to try and bypass policies.

Build effective dialogue with your staff

- Talk to your staff, understand what their job involves on a day to day basis, and try to understand their perspectives, workflow and pressures in order to learn what barriers there may be to performing certain activities. It is only by knowing about and understanding what may be preventing people from following security procedures and practices that you can work to remove those barriers. Learn from this knowledge to

help improve your systems and ensure

help improve your systems and ensure people can do their jobs effectively.

- Ensure people with the knowledge of local working environments are included in security policy making. Ensure that policies and processes are fit for purpose and proportionate, and that you provide routes for people to challenge processes that don't work well for them in practice. Organisations where people feel safe challenging the way things are done are known to be more innovative, and better able to cope with the unexpected.
- Establish processes by which issues can be reported within the organisation, and ensure that people know what these processes are and are encouraged to report issues. Build up trust within your organisation by listening to reported issues, responding positively to them in a fair manner and then involving your staff in the process of rectifying the issue. Many incidents are only ever detected by people, and if they feel they trust the organisation then they are more likely to report when they suspect something is wrong. Early detection of incidents is crucial in limiting the impact.
- Don't stigmatise mistakes and prevent individuals or teams being singled-out for blame; this will make people less reluctant to report incidents the future. Any security incident should be regarded as an opportunity for self-improvement of the individual(s) and the organisation.

Consider running security awareness campaigns

- Acknowledge that the effectiveness of awareness campaigns may take time. Allow enough time to pass before analysing the impact of any awareness work.
- Ensure that your messages are relevant to your staff and tailored to your organisation. Communicating messages that are irrelevant, unachievable or negatively impact their ways of working will not have the desired results, and may have negative impacts as it shows a lack of appreciation of your staff needs. If people are having to find workarounds to your security processes and controls to get their jobs done, then they likely already know they are breaking the rules and

more awareness isn't going to help without

more awareness isn't going to help without fixing the underlying issues.

- Focus on positive messages around what your staff can do to help, rather than just the consequences of them doing something they shouldn't. Using fear or focusing on the threats to motivate staff behaviours doesn't work well, in fact it can have the opposite effect, leaving people feeling disengaged.
- Understand that awareness is only the first step. Just because you make people aware of the risks and what to do about them, doesn't mean that they will perform those behaviours, or are able to. That could require more work to understand any technical or cultural barriers, and potentially the development of an alternative solution that works for your organisation.
- Ensure senior leadership are involved in the awareness campaign. If it's obvious that they are not following the messages (through their actions or otherwise), then this will quickly undermine the campaign's effectiveness.

Tailor cyber security training to address your needs

- Understand and prioritise the cyber security knowledge and behaviours that individuals in your organisation need before developing or procuring any training solutions. If you are looking at buying 'off the shelf' training, make sure it meets your requirements and will work well alongside your organisation's technical security controls.
- Highlight the benefits of training to your staff, be clear about how the training will help not only them, but also the organisation as a whole. This will help show your staff that they are valued by the organisation, building a sense of loyalty. Staff that care about the organisation they work for are more likely to want to help it achieve its goals, from a security perspective this may materialise, for example, through staff wanting to report necessary security workarounds they have to do in order to get their work done.
- Deliver training in small, frequent chunks. Consistent small messages are more digestible and more effective than an hour session once a year. Listen to the feedback that your staff provide about recent training

programmes, and use this information to

programmes, and use this information to adapt future programmes.

- Avoid repetition, the same training video used year after year will lead the staff to think little importance is being placed on the training. If staff think that seniors have given little thought to the training, then those participating will not be fully invested.
- Ensure trainers have sufficient knowledge of the subject and can relate it to the trainees everyday work. If trainees think they know more than the trainer (or perceive them to be out of touch), they will question the importance of the training and why they couldn't get someone more appropriate to do it. Consider asking senior management to champion the training.

Learn more

Stay Safe Online: Top Tips for Staff
The NCSC's e-learning package 'Top Tips For Staff' which can be completed online, or built into your own training platform.

CPNI security campaigns
CPNI's series of security awareness campaigns, designed to provide organisations with a complete range of materials they need.

You shape security
This guidance is for anyone looking to develop security which works for organisations and for people.

← Risk management

Asset management →

Topics

Operational security Risk management

People-centred security

PUBLISHED

11 May 2021

REVIEWED

11 May 2021

VERSION

1.0

WRITTEN FOR

Cyber security professionals

Also see

Weekly Threat Report 23rd July 2021

The NCSC's weekly threat report is drawn from recent open source...

Report
23 July 2021

The first Certified Cyber Professional (CCP) Specialism is now live!

'Risk Management' is the first certifiable specialism under the...

Blog Post
8 July 2021

NCSC statement on Kaseya incident

The NCSC's official statement on the Kaseya cyber incident.

News
5 July 2021