Cygenta

CYGENTA'S ULTIMATE GUIDE TO CYBER SECURITY CULTURE

CYBER SECURITY CULTURE: A CONCEPT DISCUSSED NOW MORE THAN EVER, BUT WHAT DOES IT MEAN?

How can we define culture in a practical way? What are the hallmarks of a great cyber security culture? And, can we measure and track it changing over time?

In this guide, we'll answer these questions and much more.

CONTENTS

If we want to influence behaviour, we must understand culture. Security culture is the foundation of security maturity in every organisation. Whether it is being actively built and measured or not, all organisations have a security culture.

Changing cyber security culture takes time, but it can be done with consistency, expertise and respect for the broader organisational culture. Cyber security awareness-raising plays a part in behavioural and cultural change, but culture is not just about awareness or behaviour, it's about values and perceptions, too. Equally important is to establish well-defined, measurable, and relevant individual and organisational metrics to measure and track culture.

Having helped hundreds of clients understand and advance their cyber security culture, we are keen to share insights that will help you. That's why we have developed a guide to help you understand how you can influence a positive security culture across your organisation. Our guide to security culture will help you learn more about:

- The fundamentals of organisational and security culture
- The importance of the human element in cyber security
- How to change your organisation's security culture
- Which metrics to use to track and measure culture
- How Cygenta's experience can help you

THE IMPORTANCE OF SECURITY CULTURE

Cyber security is a complex, multi-disciplinary topic. However, many people and organisations believe that security is about deploying layers of technology solutions enforced by strict and (sometimes) punitive policies. This is, unfortunately, a superficial approach to cyber security.

A successful approach to addressing today's evolving and complex cyber threats environment is based on three pillars – human, technical and physical. Any crack in these three pillars results in a weak cyber security posture, and all business stakeholders can feel the repercussions; partners, suppliers, and most importantly, customers.

People are the most important link in cyber security. While breaches originating from external attackers make the news headlines, most incidents can be traced back to the non-malicious behaviour of people within an organisation. We are all human, and we are all fallible. Especially when we are under pressure, being manipulated or dealing with complexity. The human element of cyber security cannot be underestimated. People play a large role in data breaches, whether it is stolen credentials, phishing attacks, technology misuse, misconfigured systems, or simply an error.

13%

of breaches due to error

82%

of breaches involves the human element

Source: Verizon Data Breach Investigations Report, 2022[1].

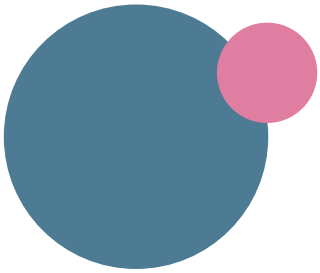
[1] https://www.verizon.com/business/resources/reports/dbir/

However, if we examine the issue more carefully, the percentage of people involved in data breaches is closer to 100%. Humans create and operate technology, and cyber incidents mostly impact humans. We haven't (yet) witnessed a case where technology attacked technology. Cyber security is about people.[2]

Our behaviour in the workplace is heavily influenced by culture. Accidental and malicious insider activity, the successful implementation of technical controls, and the likelihood of individuals reporting incidents are among the many elements your cyber security culture influences.

It is generally accepted that awareness of cyber threats drives the extent to which people practice secure behaviours. But research shows that how people feel about their organisation is just as important in driving secure behaviours as awareness of the threats[3]. The compliance budget[4] is an instinctive response rather than a conscious and explicitly calculated one: "employees fear the consequences of not being productive enough more than they fear the consequences of being the cause of a cyber security incident."

Culture is so essential to security because having a positive or negative security culture will ultimately have a significant impact on what people in your organisation recognise as normal and acceptable behaviour, which will influence how they behave.[5]



"The way things get done around here."

What is organisational culture?

MIT Professor Edgar Schein defines culture as "a set of basic tacit assumptions about how the world is and ought to be that a group of people share and that determines their perceptions, thoughts, feelings, and, to some degree, their overt behaviour."[6]

A simpler approach to organisational culture is the definition given by Deal, & Kennedy, where culture is "The way things get done around here."[7]

Although the concept of culture may sound abstract, every organisation has a culture that evolves with the organisation to fit into the changing business and risk environment. Organisational culture has a structure characterised by a mixture of tangible and intangible features.

According to Schein, culture comprises artefacts, espoused beliefs and values, and underlying assumptions. Let's break this down.

[2] https://www.cygenta.co.uk/post/the-human-element

[3] Beris, O., Beautement, A., & Sasse, M. A. (2015). Employee Rule Breakers, Excuse Makers and Security Champions:: Mapping the Risk Perceptions and Emotions That Drive Security Behaviors. Proceedings of the 2015 New Security Paradigms Workshop, 73-84

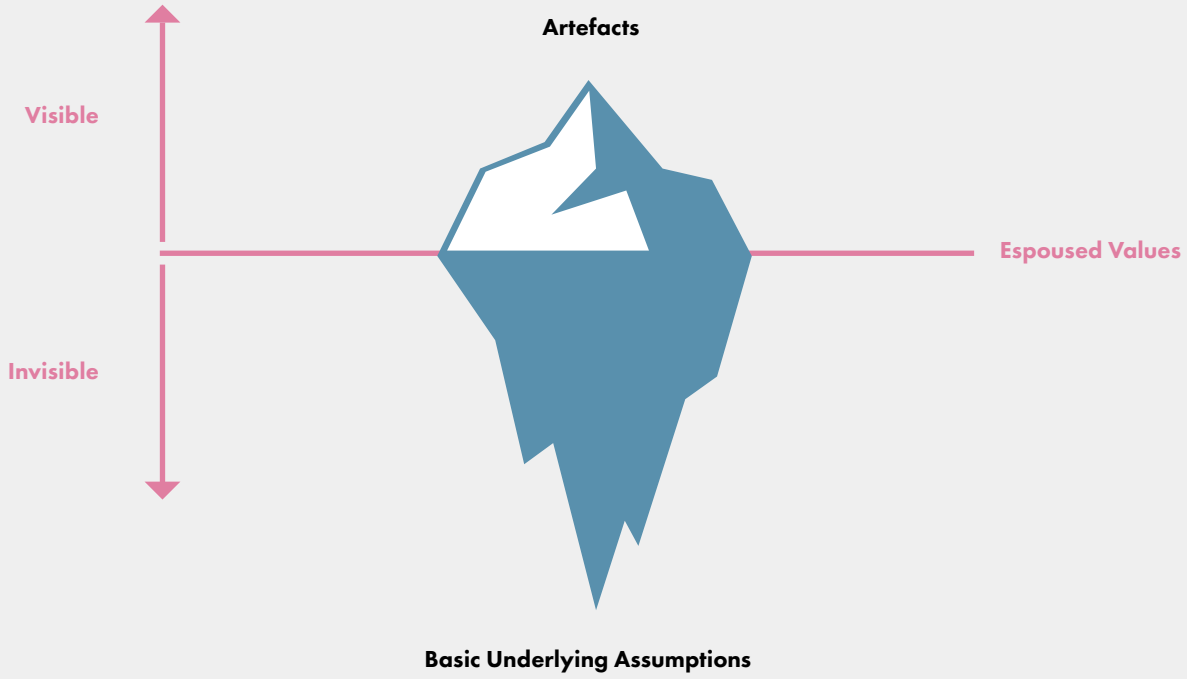
[4] Beautement, A., Sasse, M. A., & Wonham, M. (2008, September). The compliance budget: managing security behaviour in organisations. In Proceedings of the 2008 new security paradigms workshop (pp. 47-58).

[5] https://www.cygenta.co.uk/post/why-security-culture

[6] Schein, E. H. (1996). Culture: The missing concept in organization studies. Administrative science quarterly, 229-240

[7] Deal, T & Kennedy, A (2000) Corporate Cultures: The Rites and Rituals of Corporate Life. Basic Books.

Edgar Schein's model of organisation culture

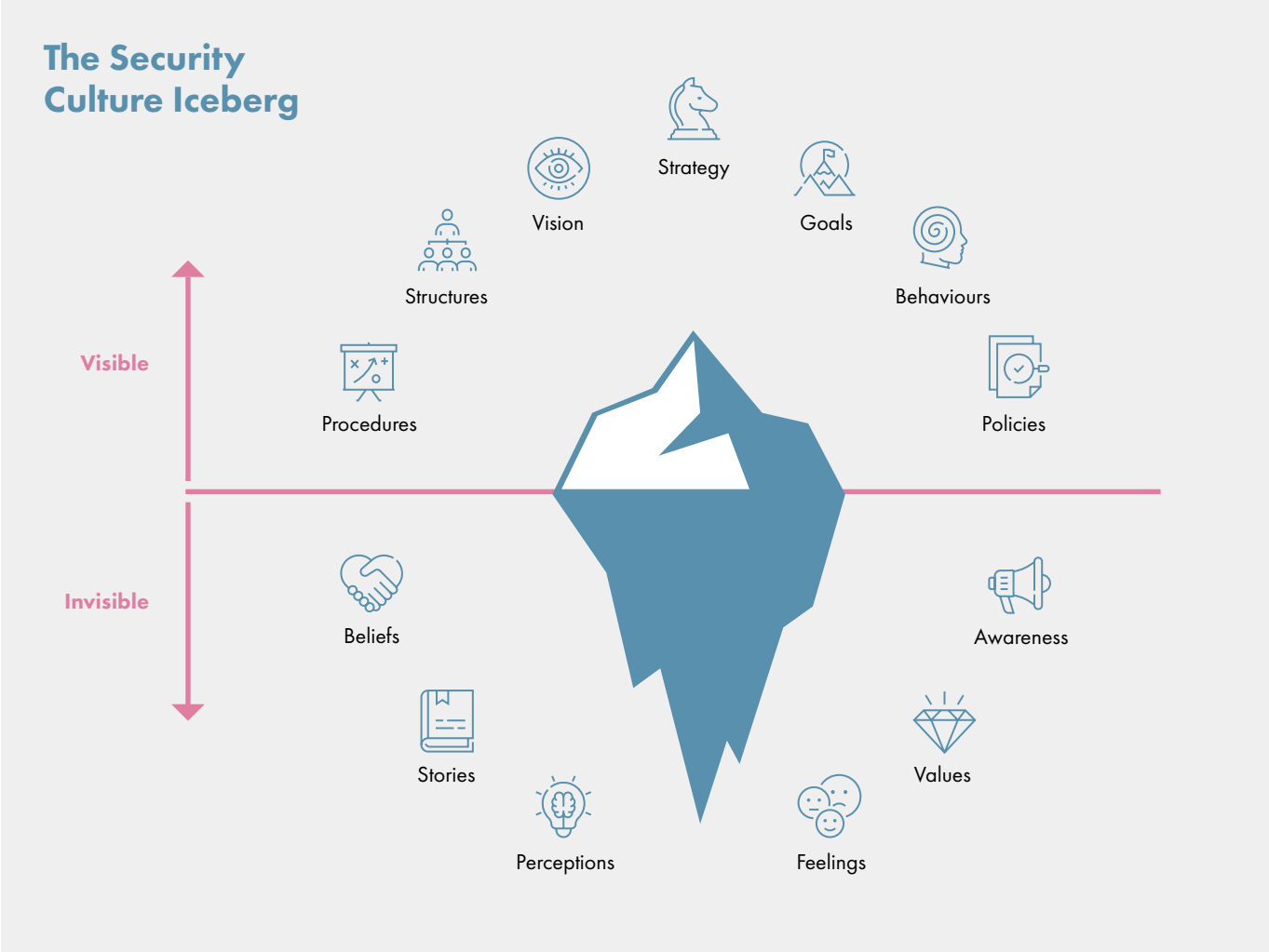


Artefacts are like symbols; for security culture, this can be branding, posters, team 'swag' etc. Artefacts are easy to see, but they are only a superficial reflection of the organization and have a limited impact on culture.

Espoused beliefs and values are what is written down. These can be statements of ideals and goals associated with values. For security, these documented statements can be security policies, guidelines, and detail of communications or training. Beliefs and values are not as accessible as artefacts but can still be seen and read. They are a representation of what we would like the culture to be, but this doesn't mean it is the reality.

Underlying assumptions are the values, perceptions, and awareness around security that are the valid drivers of employee behaviour. They reflect and inform the organisation's security culture, but they are the least visible of all cultural layers.

WHAT IS SECURITY CULTURE?



Edgar Schein's "iceberg" model of organisational culture can be adapted, as depicted in the image above, to represent the features of security culture.

Security is ultimately a social construct and is created by the different stakeholders in the ecosystem.

This reinforces what we already know: security culture is not separate from the rest of the organisational culture but needs to be in line with the wider culture.

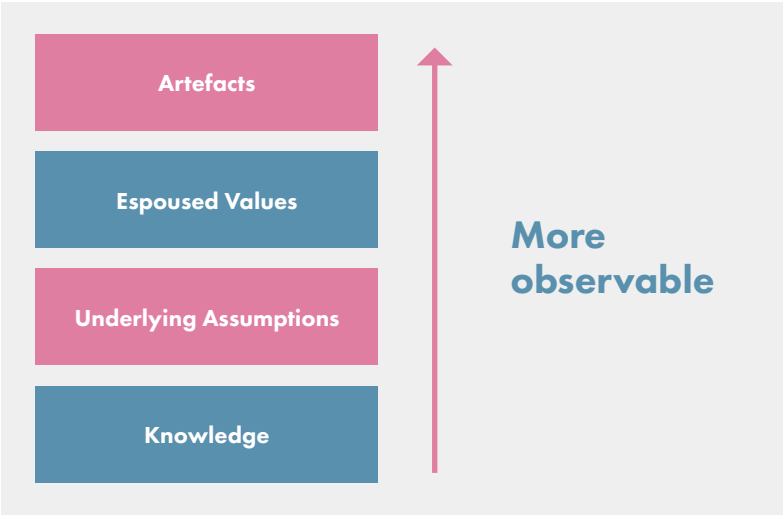
The International Civil Aviation Organisation (ICAO) defines security culture as "a set of security-related norms, values, attitudes and assumptions that are inherent in the daily operation of an organization and are reflected by the actions and behaviours of all entities and personnel within the organization."[8]

Peter Drucker coined the famous phrase "culture eats strategy for breakfast". When it comes to cyber security, we like to say, "a secure cyber security culture eats breaches for breakfast"[9]. This is because security culture is the foundation of security maturity in an organisation. It influences how people practice secure behaviours, report concerns, and ask questions. From developers engaging with the security team to how you handle an incident: security culture is the linchpin.

[8] https://www.icao.int/Security/Security-Culture/Pages/default.aspx
[9] https://www.youtube.com/shorts/vDE6NCWskdU

Besides the three core features of organisational culture, in cyber security we can add a fourth layer of knowledge, in the sense that knowledge influences the assumptions, values, and behaviours related to security.[10]

Knowledge could be understood as 'awareness.' Since values and assumptions are often the more difficult layers to observe, understand, and influence, many focus on awareness/knowledge and behaviour when speaking of a cyber security culture. Although these are important, assumptions and values are the more impactful.



SUB-CULTURES

Within any culture, there are sub-cultures. The cyber security culture in your IT team will differ from that of your developer community, which again will differ from your marketing team.

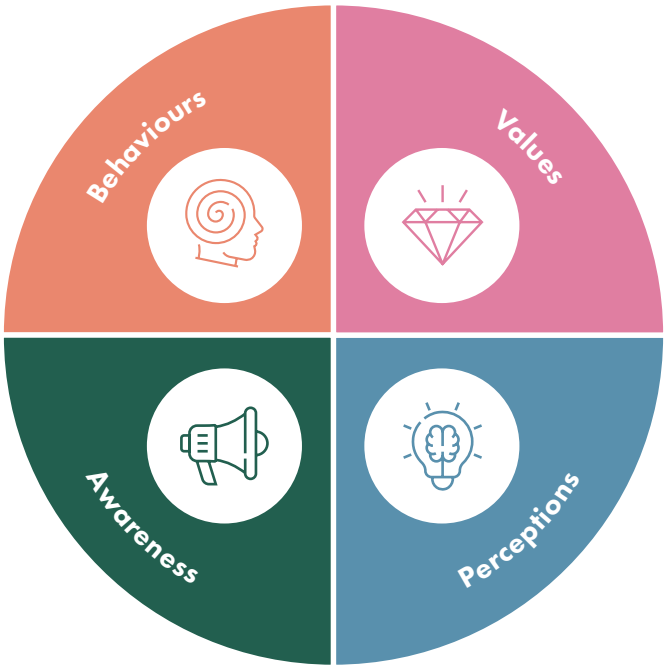
All functions will be influenced by the wider organisational culture, but they also belong to their own sub-cultures. This will inform their values, perceptions, awareness, and behaviours. When measuring and tracking culture, it's important to keep this in mind, for example when it comes to data collection and analysis. Tailored training and communications can be very powerful when reaching different sub-cultures, for example many of the organisations we work with have a programme of technical champions to motivate and engage their developers.

[10] ENISA (2017). Cyber Security Culture in Organisations. European Union Agency For Network and Information Security. Available at https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

CYGENTA'S CYBER SECURITY CULTURE FRAMEWORK

Cygenta's cyber security culture framework draws on the great academic research and our experience working with the cyber security programmes of hundreds of clients around the world.

At Cygenta, we define cyber security culture as comprising four key areas: **Values, Perceptions, Awareness** and **Behaviour.**



VALUES

How closely the security values match the organisational values is very important. If security values contradict organisational values, security will suffer in the end. People will resist change and the imposition of values and procedures that clash with priorities they know are more important to the business. This will lead to cognitive dissonance and a gap between what is said about security and what is practised day-to-day. In the long run, such gaps will damage the security culture.

For example, let's take an organisation with a culture built on positivity and putting people first. If the security team penalises people for making mistakes and enforces controls without explaining the 'why', they will be alienated from the rest of the company. Their colleagues will avoid coming to them with problems, and they may find themselves viewed as an ivory tower. In this case, it is, therefore, important to align the security approach with the wider positive organisational culture to support and safeguard people and reinforce a no-blame culture based on trust.

Values are closely related to the attitudes and beliefs of employees. Whether people have a positive or negative opinion about security (their attitude) is formed through experience, education, and observation. Those around them also influence it. Do people feel a level of responsibility for cyber security, or do they feel that it is the job of the IT department?

PERCEPTIONS

Many extrinsic and intrinsic factors can influence people's perception of cyber security.

Fear-based vs. empowering security culture

An organisation may have a negative or a positive security culture (or anywhere between). A negative, fear-based security culture will alienate people. When it comes to security culture, we have much to learn from the aviation industry and how they treat incidents.[11] The aviation industry understands that blaming people doesn't reduce incidents; it just reduces your likelihood of knowing about them. And this is the last thing we want in cyber security.

If we have a culture of fear, then people don't make less mistakes. They just don't report them. Lack of timely reporting means that organisations will have less time to react, investigate the incident and remediate it to minimise impact.[12]

On the other hand, a positive, empowering security culture engages your employees. They will feel safe to report an incident, even if they caused it. Security becomes part of their job description and not somebody else's responsibility. There is a shared belief that security is an enabler of business success, not a barrier to productivity and innovation.[13]

HOW CAN YOU REWARD AND REINFORCE POSITIVE SECURITY BEHAVIOURS TO IMPROVE PERCEPTIONS?

- Share a digital thank you note for security engagement
- Find a way to recognise people who report incidents & phishing tests
- Create a champions programme to extend the friendly eyes, ears & voice of security
- Review your incident process - do you give feedback to the reporter? How do you offer emotional support to anyone who has been negatively affected by an incident?
- Shine a light on the security team itself, highlight hard work and achievements

[11] https://www.tripwire.com/state-of-security/aviation-safety-cybersecurity-learning-from-incidents
[12] https://www.youtube.com/watch?v=-Xy4y-cm83I
[13] Spitzner, L. (2021). Why a Strong Security Culture? SANS. Available at https://www.sans.org/blog/why-strong-security-culture/

In other terms, what you should be looking for is establishing a restorative Just Culture. A restorative Just Culture enables organisations to learn from incidents while holding people accountable for poor performance.

It is forward-looking and looks at the deeper conditions that facilitated the incident, focusing on what went wrong rather than who can be blamed. On the other hand, a retributive Just Culture focuses on individuals, seeking to place blame and administer punishment.

A restorative Just Culture recognises that emphasising individual blame and punishment does not reduce the likelihood of incidents, it simply reduces the likelihood of people reporting incidents and therefore undermines opportunities to identify issues and learn from them.[14]

Perceptions of others

Social proof is an essential factor shaping our behaviour: when we are unsure of how to behave, we look to people with influence or authority to mimic their behaviour. So, how people in authority act influences how others throughout the organisation perceive security. For example, if team members see their line manager sharing passwords and using WhatsApp to share customer data, they will likely perceive this as accepted behaviour – regardless of what company policies may say.

[14] Dekker, S. (2012) Just Culture: Restoring Trust and Accountability in Your Organisation Ashgate: England

CHAMPIONS

Security champions are people throughout the business who don't work for the security team, but they become the friendly voice and ears of the security team in their teams. When set up for success, a champions network can be a great way to supercharge your security culture, tapping into social proof. Champions can help to:

- scale up awareness-raising
- increase incident reporting
- understand how different teams feel about cyber security
- identify gaps in security guidance, policy and practices
- improve perceptions of security throughout the business

There are challenges to setting and running a champions programme, for example it's important to consider time commitments, workload, communications, and incentives. But, when you get a champions programme right, it pays off dividends.

When it comes to security culture, perceptions of the security team are essential. What is the view that employees have of the security team? Is it the 'department of no', or is it there to support their job and initiatives? This perception will influence whether people engage with security on their projects, ask questions and report incidents.

Perceptions of themselves

Self-efficacy – a person's belief that they can successfully execute the recommended behaviour to reach a desired outcome – has long been regarded by psychologists as the most important factor in behavioural change.[15] Self-efficacy is a reliable predictor of cyber-security intention and behaviour, and interventions that seek to improve self-efficacy among people are more likely to yield positive results than those which merely stress the cyber security threat.[16] Raising awareness of threats is, of course, fundamental, but it will only take your cyber security culture so far. Empowering people, raising their confidence and giving them the tools to practice more secure behaviours is the true game-changer.

AWARENESS

Awareness can have different meanings in different settings. However, cyber security awareness can be defined as "focusing individuals' attention on protecting against the criminal or unauthorised use of digital data so that they can respond accordingly.[17]"

One of the biggest concerns for organisations is criminals manipulating unwitting people through social engineering attacks or taking advantage of human error. To better protect individuals, organisations, and communities, we need to raise cyber security awareness. Awareness in organisations is important for mitigating malicious as well as non-malicious insider activity; the more people are aware of cyber security, the more malicious activity is likely to be identified before impacting organisations and people.

The Cygenta engagement equation

However, cyber security awareness alone is not enough to change behaviours. Organisations need to understand why certain behaviours are practised (or not) for awareness to be meaningful. Understanding the cultural 'why' helps to explain the behaviours you seek to influence. There are no 'irrational behaviours', only behaviours we cannot explain due to the lack of awareness of the cultural context.

'Why' helps us frame cyber security in a more impactful way. But that is only half of what we at Cygenta call the "cyber security engagement equation.[18]"

[15] Bandura, A. (1977) 'Self-efficacy: Toward a unifying theory of behavioural change' Psychological review, 84(2), 191-215
[16] ENISA (2018) Cyber security Culture Guidelines: Behavioural aspects of cyber security
[17] Barker, J., Davis, A., Hallas, B., Mc Mahon, C. (2021). Cyber security ABCs: Delivering awareness, behaviours, and culture change. BCS Learning and Development Ltd.
[18] https://www.cygenta.co.uk/post/cyber-security-awareness-50000

Cygenta's Cyber Security Engagement Equation

The second half of the equation tackles 'why me?'. This provides the context, helping people understand not just why cyber security is relevant but why it is relevant to them. Without this, it is hard to influence people's intrinsic motivation, and this is key to influencing behavioural change.

For a cyber security awareness campaign to be successful, it should seek to improve behaviour and strengthen the cyber security culture. If we want security awareness to be effective, it should engage in shifting the understanding of cyber security to such an extent that it positively influences behavioural change.

BEHAVIOUR

Cyber security behaviours are influenced by – and influence - values, perceptions, and awareness. It's an iterative process. It is essential to understand that although the security behaviour definition may differ, the common denominator is that employees are involved in actions related to increasing or reducing the cyber risk to the organisation.

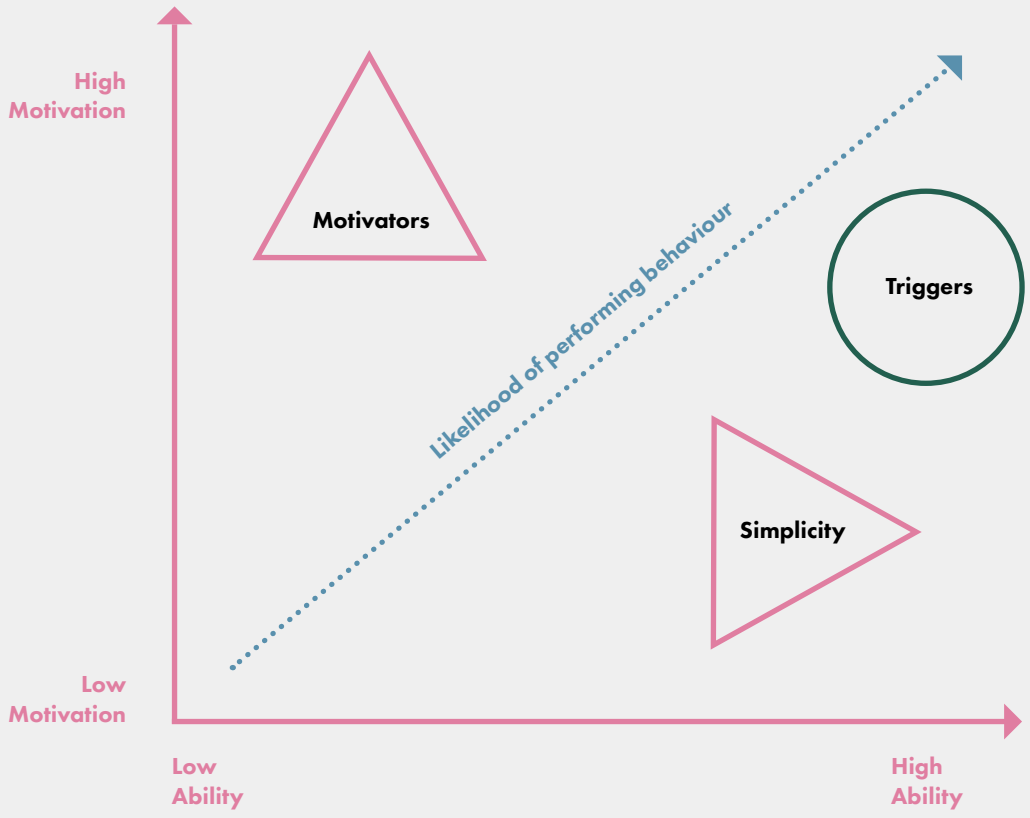
How to use behavioural models

When planning and delivering cyber security culture programmes, there are two behaviour models which are particularly helpful.

B J Fogg's **B=MAP** behaviour model[19] stresses the importance of **motivation, ability,** and **prompts** when influencing behaviour. According to this model, if a behaviour is lacking, one of these aspects is missing.

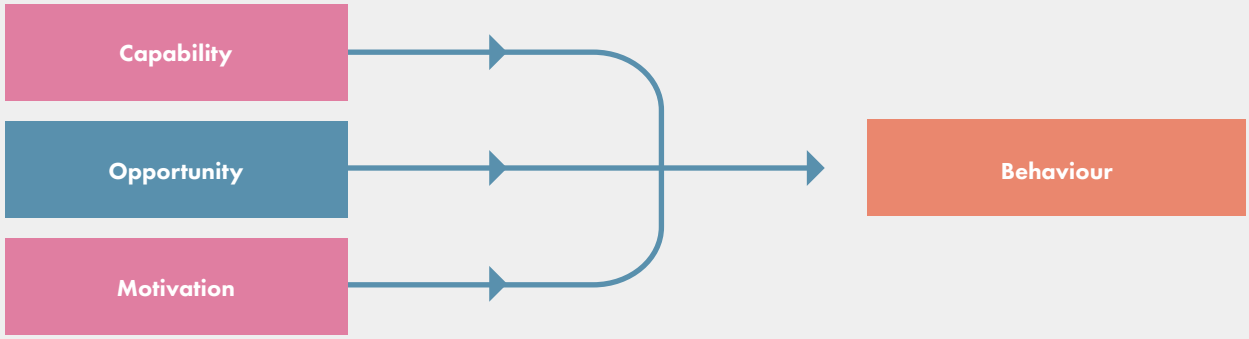
Susan Michie's **COM-B** model suggests that **capability, opportunity,** and **motivation** are the drivers of behaviour change[20]. Capability is the knowledge and skills people have. Opportunity is whether people have the time to change their behaviour and whether the norms and values of their surroundings encourage them. Finally, motivation is examining if the behaviour change aligns with their values and beliefs and if it is something that can become a habit.

B J Fogg's B=MAP



[19] https://behaviormodel.org/
[20] Michie S., van Stralen MM., West R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implement Sci. doi: 10.1186/1748-5908-6-42

Michie's COM-B model



ENISA suggests[21] that the COM-B model is used to identify why a desired behaviour may or may not be carried out and that Fogg's behaviour model guides thinking about possible interventions. Let's consider an example to bring this to life. If you are trying to drive the use of a password manager across your organisation, but engagement is low, you can first consider the COM element of Michie's model:

- Do people have the capability to use the password manager?
    - Is it accessible, and has good support been provided to train people and continue to guide them?
    - Is it as easy as possible for people to engage with?

- Do they have the opportunity?
    - Have your colleagues been given time to become familiar with using the password manager? Are they under pressure to be particularly productive, increasing the friction of setting up and using a new system? Is the use of the password manager supported 'top down', to drive the accepted norms of behaviour?

- Are your colleagues motivated to use the new password manager?
    - Has there been a strong awareness campaign to drive the use of the password manager, including the engagement equation?
    - Are you using principles of social proof, for example, via support from a champions programme, to drive motivation?

With the answers to above in mind, you can then draw on Fogg's B=Map to plan interventions:

- If you have identified that motivation is lacking, you can develop a strong awareness campaign to answer 'why?' and 'why me?'

- If ability is an issue, you may want to hold some workshops to understand where there are blockers or distribute step-by-step, engaging guidance.

- If opportunity is a blocker, it might be time to get senior stakeholders on board, including an awareness campaign targeted at them. You can also consider whether people have been prompted to change their behaviours. Prompting people at the right time can be a game-changer, for example, when people send a password reset request, you could nudge them in the direction of your password manager so that they can see the tangible benefit.

Behaviour change becomes a lot easier when the new behaviour is made as simple as possible to practice, when people are motivated to change their habits and when they are prompted at the right time.

When behaviour models are not the answer

Behaviour models can be helpful, but it is important that we don't simply focus on individual behaviour. People often engage in security 'workarounds' or insecure behaviours when security policy is regarded as unrealistic or at odds with the wider values of the organisation. For example, if the organisation values productivity very highly, then security processes that take more time can be bypassed because they are seen as conflicting with productivity. In these cases, streamlining processes, consulting different parts of the business, or changing the policy will generally be more appropriate and impactful than trying to change employee behaviour.

HOW TO MEASURE SECURITY CULTURE

Although many argue that security culture cannot be measured, this is far from true. There are many opportunities to build and track cyber security metrics. One approach we take at Cygenta is to consider key areas of security culture, analyse how individuals behave in relation to these areas and examine how this changes according to training, other communications, policy, and system changes.

Data analysis, surveys, focus groups, document reviews and observational analysis can all have their place in measuring security culture.

Using data and surveys can help identify what is going well and where there are challenges; focus groups are unrivalled for exploring why challenges persist and how to tackle them. For example, data may highlight that many people in a company are clicking links in phishing simulations and not reporting them. A survey may then show that people have a good level of awareness regarding the risks of phishing. And then focus groups can identify the root causes behind these findings.

For example, people may receive many legitimate internal emails with the hallmarks of phishing or a very high volume of internal emails. Or, focus group discussions may indicate that people may be scared to report phishing emails when they have clicked on them because they fear punishment.

Metrics to measure

For metrics to be truly insightful, they must be specific, well-defined, measurable, and relevant. When defining your metrics, it is so important to consider the second-order impact of metrics – e.g., just focusing on click rate can make people scared to click anything and, therefore, less productive. Spotlight the behaviour you want and provide positive reinforcement.

Individual behaviour metrics can include:

- Simulated phishing report rate
- Percentage of crackable passwords
- Time to install updates
- Time spent on password resets
- Reported rate of self-efficacy

However, when it comes to measuring security culture, it is a common trap to focus solely on individual behaviour metrics. While these data points have their place, security culture is not just about what people do, it's about what the organisation prioritises and supports.

With this in mind, some organisational metrics include:

- Scale of password manager roll-out
- Time required to respond to incident reports
- Percentage of incident report feedback
- Frequency of awareness-raising comms
- Reported perceptions of executive buy-in

To build a positive and proactive security culture, it is important not to approach metrics as a way to attribute blame to people. Instead, metrics are best viewed as a means to understand what works, and what doesn't, to identify behaviours that you would like to change, measure these behaviours, conduct an awareness-raising activity, and then measure again.

You could consider the following five ingredients in building a positive, proactive security culture.

Five security culture goals

✕ Forget click rate	✓ Focus on report rate
✕ Out with long list of 'don't do'	✓ In with key call-to-actions
✕ Don't dismay with walls of text	✓ Do delight with bitesize videos
✕ Break the shackles of fear uncertainty and doubt	✓ Build foundations of self-efficacy
✕ Abandon naming and shaming	✓ Embrace a 'no blame' approach

Indicators of a Positive, Proactive Security Culture

When we're running a cyber security culture assessment, indicators of a great cyber security culture that we look for include:

Incident report rate
As culture improves, this generally rises because people are more attuned to incidents and more comfortable reporting problems & concerns. As the security culture matures, the rate of incidents then generally decreases.

Feedback process for incidents
When people report incidents or issues, do you let them know the outcome? It has a big impact on future behaviour to close the loop on this & provide positive reinforcement.

Tone from the top
This is social proof 101. Do senior executives send the right messages about cyber security *and* model the behaviours you are trying to promote? Do they own it?

Reported rates of self-efficacy
Self-efficacy matters more than awareness of threats. Do people feel confident that they can engage in the cyber security practices you are trying to build? Or do they think they haven't got the time, capacity, skills or incentives?

Restorative Just Culture baked into company values
The big one when it comes to whether people will report incidents or brush them under the carpet. When there's an incident, do you look at what went wrong or who you can blame?

KEY TAKEAWAYS

If you take one message away from this guide, we hope it is the power of a positive and proactive cyber security culture. People are often described as the weakest link in cyber security, but this is not true. We are the only link. It is people who design, develop, configure, use, and abuse technology. People are so often the strongest link in cyber security, especially in the context of an empowering culture which takes account of how we, as human beings, reach decisions and change our behaviours.

Culture is more than awareness.

It's more than behaviours. It is also the shared values and perceptions that influence what people believe about themselves, their colleagues, and the organisation as a whole.

Cyber security culture can be measured and tracked.

Your organisation already has a cyber security culture, whether it is being actively built and managed or not. It is the foundation of security maturity, influencing behaviours at all levels and in all teams.

Positive culture change takes time and work.

It does not happen overnight, and it can be demanding. But it is so rewarding. When you have a strong cyber security culture, it makes your job as a security practitioner not only easier, but also more enjoyable and impactful. The positive ripple effect of your work will spread beyond the boundaries of the company you work for. Your colleagues will be safer online, both at work and at home.

THE CYGENTA OFFERING

At Cygenta we don't just do cyber security. We navigate you through cyber risk. Some of our Human Cyber services, that may interest you, include:

Cyber Security Culture Assessments

We help you understand where there are gaps in security policies and day-to-day behaviours, why these gaps exist and what you can do to close them.

Our in-depth analysis and practical reporting provides tailored recommendations and metrics you can apply to advance your security culture and mitigate human cyber risks in your organisation.

Our cyber security culture framework has been developed over more than a decade of working on cyber security awareness, behaviour and culture programmes with organisations in sectors that span government, defence, financial services, retail, healthcare, telecoms and more.

We navigate the different layers of your cyber security culture to explore four key areas: values, perceptions, awareness, and behaviours. Within these four areas we explore:

- Perceptions of leadership
- Evidence of a 'just culture'
- Levels of personal responsibility
- Levels of self-efficacy
- and much more

Cyber Security Awareness Raising

We offer packages of collateral that you can use throughout an engaging, comprehensive awareness-raising campaign.

How a Hack Works is our most popular package. Rooted in demonstrations of cyber attacks, this pack of content demystifies cyber security, bringing it to life. The package centres on six bitesize awareness videos that will get your whole organisation talking about cyber security.

How a Hack Works bitesize videos:

- **Cyber-crime explained**
- **Hacking humans**
- **Phishing in action**
- **Hacking passwords in action**
- **Ransomware in action**
- **The dark web uncovered**

If you are looking for bespoke videos, let us know the topics you want us to tackle, and we'll make tailored videos for you and your colleagues. We'll bring our expertise to bear on the script and delivery. You will have the opportunity to review the development of the product at every stage. Together, we will make something that we'll all be proud of - and that your colleagues will relate to and engage with.

Champions

The Cygenta Champion Leader Framework equips you with everything you need to build and run a sustainable, successful cyber security champions network from scratch.

Detailed guidance takes you through every stage of setting up, measuring and maintaining a champions programme in your organisation. Complete with resources and templates that enable you to tailor the programme for your organisation at every step of the way.

Check out our online course at academy.cygenta.co.uk or get in touch to discuss your needs.

"The Cygenta Champion Leader Framework has been invaluable"

Admiral

"If you're looking for a team to deliver a powerful cyber security awareness message, then look no further than the team at Cygenta"

Bell Canada

"Cygenta can be trusted to understand complicated issues and look at problems from different angles"

Titania

For more testimonials, visit www.cygenta.co.uk/clients

ABOUT US

Cyber security is often treated as a series of single problems delivered as a series of single initiatives. In 2017, husband and wife team Dr Jessica Barker and FC founded Cygenta out of frustration with this narrow approach to cyber risk. At Cygenta we believe that the best, sustainable defence against threats has to consider all aspects of security risk. With more than 30 years combined experience across a wide field of sectors, our co-founders are driven by securing the success of more than 250 clients globally.

OUR APPROACH

Our approach to cyber security is more than just penetration testing or awareness training. We are experts in combining the technical, human, and physical aspects of security best practice.

We help some of the largest and most complicated organisations build resilience and sustainability in their risk management, not just their technical response.

Our unique combination of technical, human and physical risk services are delivered step-by-step according to your needs and maturity level. We start with the fundamentals of vulnerability scans and then build to cultural assessments and change management support. And we don't just disappear after each step. We want to help you build ongoing resilience as new threats emerge.

In short, we care.

If you have any questions or would like to find out how we can work with you, please get in touch.

Contact us:

www.cygenta.co.uk

Follow us:

@CygentaHQ

linkedin.com/company/cygenta

youtube.com/cygenta