

BUILDING A CYBER-RESILIENT CULTURE

AN ORGANISATION-WIDE JOURNEY TO COMBAT EVOLVING CYBER THREATS



INTRODUCTION

As the cyber risk landscape evolves, executives are increasingly questioning how well their businesses are protected: Do we have the right risk assessment framework to identify threats early? Are our anti-virus software and encryption solutions strong enough to protect against the latest threats? But one question they often forget to ask is: How much do our own staff care about cyber threats in their day-to-day roles?

Tools, frameworks, and controls to guard against malicious actors only address one aspect of cyber risk. Even with these in place, employees – with or without malicious intent – may still expose the organisation to threats. Data breaches need not always be the result of expert hacking or malware attacks on data servers. They can also occur if an employee forgets to lock his or her laptop and a third party then steals their credentials and gains access to confidential data. **5 billion records were stolen or compromised in 2018, of which over 2 billion were stolen as a result of insider circumstances**¹. To truly protect an organisation, it is therefore also important to build a **cyber-resilient culture**.

The degree to which a corporation is cyber-resilient will reflect its broader, fundamental organisational culture. This can lie on a spectrum ranging from one where employees take a dismissive rules-don't-matter-to-me attitude to a culture where everyone is involved in making the business more risk-aware². To make progress in this respect, organisations need to put in place mechanisms to inculcate cyber-resilient behaviours as part of a long-term journey, similar to any large scale culture change.

A CYBER-RESILIENT CULTURE is a state of maturity in which all staff make conscious efforts to **behave in ways that protect the organisation** against cyber threats; and in which they are supported by **appropriate mechanisms** to inculcate the required behavioural changes



¹ Risk Based Security, Inc. (2018). Data Breach QuickView Report, 2018 Data Breach Trends

² Oliver Wyman (2014). Getting to the heart of risk culture within Financial Services

A CYBER-RESILIENT CULTURE VERSUS OTHER CYBER MEASURES

Organisations are rushing to build their cyber defences in response to their increasingly digitised business operations and the prevalence of cyberattacks in the news. Common measures include a comprehensive cyber-risk strategy with a suitable operating model; a dedicated cyber risk appetite statement (RAS); an automated cyber-risk dashboard; tightened security controls; a quantified cyber value-at-risk measure; and the building of a robust, cyber-resilient culture. This has led to debates over fundamental questions such as how to balance the hard and soft aspects of cybersecurity. These often lead to the following pitfalls:

1 *Let's de-prioritise culture for something more concrete*

Many executives are rediscovering the differences between integrating cybersecurity mechanisms and building a cyber-resilient culture. They typically focus more on the former task, often as an add-on to other initiatives and with the intention of achieving quick wins. But they then realise that cyber risk is a bigger problem and cannot be tackled by cybersecurity mechanisms alone.

The truth: the number of security tools you have does not guarantee the safety of your data or protect your business³. Moreover, changing the culture – building a cyber-resilient culture – takes much longer than implementing security controls, so it requires organisations to start sooner rather than later.

2 *Our defence against insider threats is already good enough. What we need is protection against external attacks*

Nearly 75 percent of companies believe they have appropriate controls to mitigate internal staff threats – but more than 50 percent of companies had a confirmed cyber incident in the past 12 months due to actions by staff⁴.

3 *Cyber attacks always involve sophisticated, technical approaches*

The boards of too many companies still pick up most of their information about cyber events from media, which often report on the more-sophisticated forms of attacks, such as ransomware and malware. In fact, a data breach is more likely to result from an employee leaving a laptop on a train than from a malicious criminal hack⁵.

3 Microsoft (2018). Cybersecurity in APAC: The art of simplicity and being on the right side of history




4 Oliver Wyman (2019). The Increasing Threat from Inside

5 Insurance Journal (2017): Effective Cybersecurity Strategy Rests on People, Not Just Technology

While frameworks are value-adding and critical, they will be less effective in the absence of a **robust cyber-resilient culture**. Frameworks may inform and help address some high-risk issues, but it is the culture that helps minimise the occurrence and impact of cyber issues, ensuring business continuity. Security tools can close as many doors as possible, but it is the robust cyber-resilient culture which ensures that staff follow the rules and do not find loopholes in the controls ecosystem.

To illustrate this point, we provide some examples of how staff across various teams can bypass hard security controls, demonstrating poor cyber behaviour and exposing the organisation to cyber threats. (See Exhibit 1.)

Exhibit 1: Poor Cyber Behaviour Examples (illustrative)

STAKEHOLDERS AND DAY-TO-DAY ACTIVITIES	DEMONSTRATED BEHAVIOURS	POTENTIAL IMPACT
 <p>JOSH IS A MID-CAREER HIRE WHO WILL UNDERGO NEW-JOINER TRAINING ONLY IN 3 MONTHS' TIME</p>	<p>Unknowingly bypassed cyber protection measures and transferred files from personal USB device</p>	<ul style="list-style-type: none"> • Josh's personal USB device contained a malware-infected portable file application • When plugged in, the malware was downloaded on and infected his computer • The malware encrypted specific files and folders in the shared drive of the department, preventing internal access to the files • This impacted 2,000 endpoints within a critical team of the organisation
 <p>AVINASH IS A FINANCE STAFF WHO IS RECEIVING PUSH NOTIFICATION ON SECURITY UPDATES</p>	<p>Ignored notification and kept pushing out the updates</p>	<ul style="list-style-type: none"> • As a security update had not been performed in a timely manner, the software environment had vulnerabilities that exposed it to cyberattacks • The hackers were able to gain access and install a malware, enabling them to monitor the organisation's payment transaction process and understand the internal processes • After months of gradual planning and build-up of undetected attacks, the hackers finally gained enough access across different points of approval to submit a substantial size of fraudulent transactions • The hackers were able to channel high-value transactions to unauthorised accounts, deleting their trail of attack (from the automated reconciliation report), making it difficult for the organisation to detect the unauthorised activities
 <p>LORENA FROM THE COMPLIANCE TEAM HAS JUST RETURNED FROM A VACATION AND IS CLEARING HER INBOX</p>	<p>Failed to exercise cyber awareness and clicked on a socially-engineered/ personalised phishing mail</p>	<ul style="list-style-type: none"> • Having entered her user login credentials and clicked on the link in the phishing email, Lorena had (unintentionally) provided hackers with access to high-level privileges in the bank's systems – including multiple critical databases and internal systems • The hackers were able to cover their tracks and attacks were undetected for a considerable duration • Over a 1-year period, the hackers stole over 1 million sensitive customer data (such as identity card and credit card information) and released that to the public

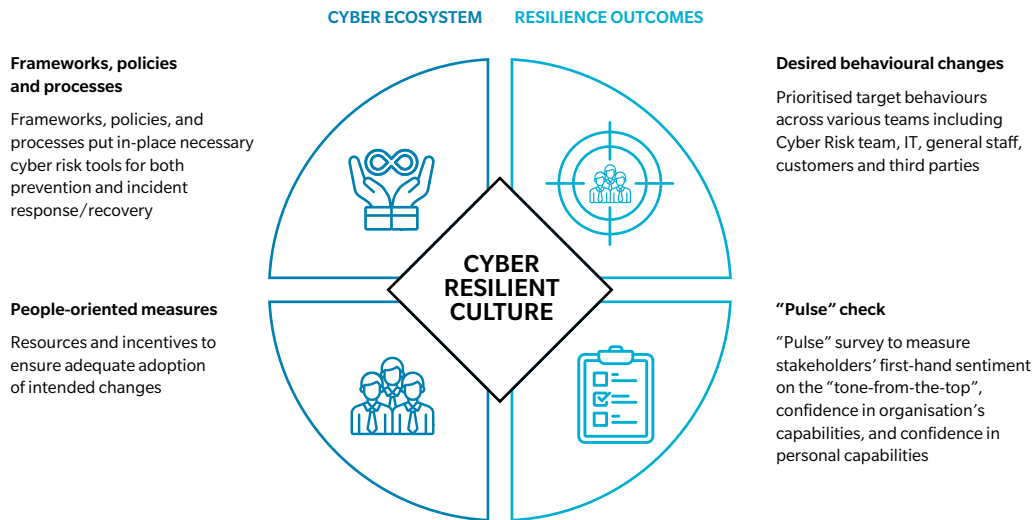
Reading these examples, we quickly see that unless staff are trained to behave in a cyber-resilient manner, the organisation will continue to be exposed to significant cyber risks. However, the question corporations should ask is: **“How do we make staff realise that their actions could pose serious risk to the organisation and that some changes are necessary?”**

The answer is to build a robust cyber-resilient culture. In subsequent sections, we describe our approach to this and to measure progress over time to ensure that the organisation is moving in the right direction. It is important to note that it takes time to change culture. Organisations should view this as a continuing journey instead of a one-off fix.

BUILDING A CYBER-RESILIENT CULTURE

As described, a robust cyber-resilient culture is one where all staff **behave in a way that protects the organisation** against cyber threats, supported by **appropriate mechanisms**, to inculcate the required behavioural changes. This needs a fully coordinated approach across four dimensions, as shown in Exhibit 2. On the left side is the **cyber ecosystem**, which establishes frameworks, policies, and processes. These are combined with people-oriented measures, which act as reinforcing structures to drive adoption. On the right side is a set of **resilience outcomes**, aimed at ensuring that the resulting behavioural changes and stakeholders’ mindsets are moving in the right direction.

Exhibit 2: Four Aspects Of A Cyber-Resilient Culture: Ecosystem And Outcomes



While all four aspects are necessary to achieve true cyber-resilience, the most-crucial task for deciding the direction of the culture-building journey is to identify the **desired behavioural changes**. (See Exhibit 3.) This sets an organisational rhythm in which staff can demonstrate those behaviours.

Exhibit 3: Examples Of Desired Behaviours According To Day-to-day Responsibilities

DAY-TO-DAY JOB ACTIVITIES

- Check emails
- Browse internet
- Connect with friends/colleagues on authorised communication service
- Use office computer/laptop to access customer data or other confidential information to carry out day-to-day responsibilities

PRELIMINARY LIST FOR PRIORITISED BEHAVIOURS

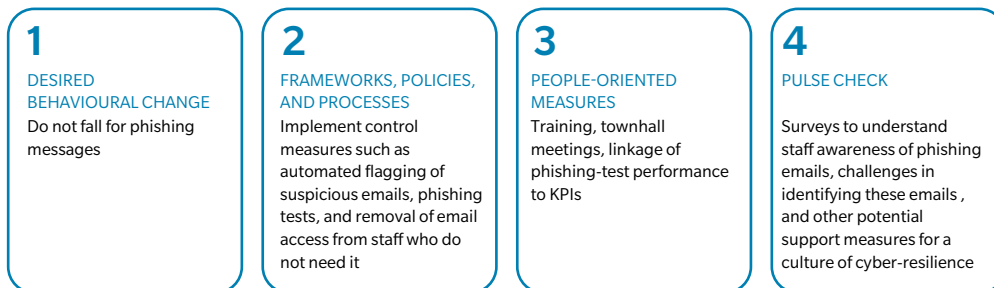
- 1 With every suspected email, ask yourself “do I know the sender?” or “what are they asking from me?”, before clicking on any link. When in doubt, report the suspected phishing email to relevant IT security team
- 2 Be aware of malicious websites and do not access them
- 3 Use only authorised communication services/applications
- 4 Protect customer information and internal data at all times – lock computers, set strong passwords, only share information on need-to-know basis
- 5 Take cyber-related learning and training seriously and allocate time to complete the training as soon as possible
- 6 Protect personal passwords and do not disclose them to any personnel, including the IT department

A defined set of **desired behavioural changes** informs the **frameworks, policies, and processes** required to lay down the standard for what is considered as an undesirable behaviour or a breach of a desired behaviour. **Training, incentives, coaching, and communications** can then be rolled out to ensure adequate adoption of and compliance to these agreed standards. Finally, a **pulse check** provides insights into progress and gathers feedback that can be used to make improvements where needed.

For example, one commonly desired behaviour is for employees not to fall for phishing messages. The following measures can drive this change:

- Introduce control measures, ranging from the automated flagging of suspicious emails to the removal of email access from staff who do not need it.
- Conduct a periodic phishing test to measure staff awareness.
- Introduce people-oriented measures, such as training and educational townhall sessions with team leads.
- Eventually, link performance in phishing tests to employees’ key performance indicators (KPIs).
- Take pulse-check surveys to understand how well staff know how to deal with phishing emails and the challenges they face during phishing drills. The surveys can also point to possible additional support that might strengthen the culture of cyber-resilience.

The four keys to building a culture of cyber-resilience:







It is imperative for organisations to identify, establish, and communicate a defined set of desired behavioural changes. Doing this will promote building of a cyber-resilient culture from scratch.

KNOW THYSELF IN THE CULTURE-BUILDING JOURNEY

Strengthening cyber resilience is a long journey, and it is important to measure progress so as to ensure it is going in the right direction and has sufficient impact. This requires a set of measurement metrics that collectively track progress across all four pillars of the cyber-resilient culture described in Exhibit 2.

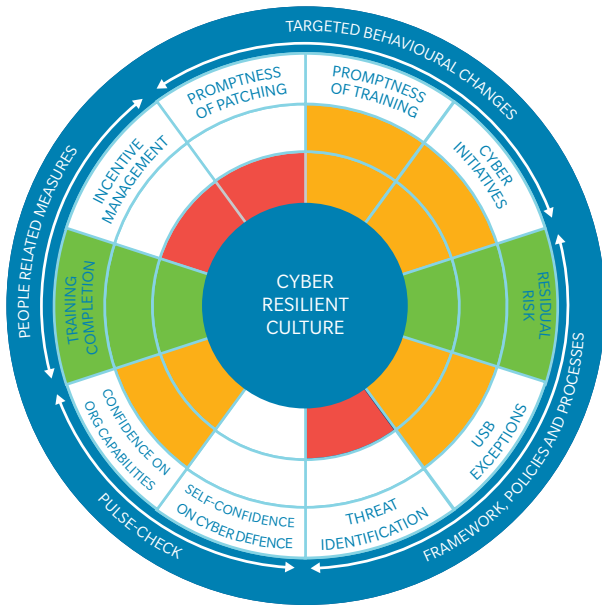
Exhibit 4: Illustrative Set Of Metrics

PILLAR	METRICS' DETAILS	EXAMPLES
FRAMEWORK, POLICIES, PROCESSES 	To gauge the effectiveness of frameworks, policies, and processes in setting up a cyber-resilient culture by measuring items such as residual risk, breaches, and exceptions	<ul style="list-style-type: none"> Number of business partners onboarded without cybersecurity checks Percentage of staff with approved exceptions to use USB sticks Number of systems with high residual risk
PEOPLE-RELATED INITIATIVES 	To evaluate the effectiveness of people-related initiatives in strengthening a cyber-resilient culture by measuring the comprehensiveness of these initiatives	<ul style="list-style-type: none"> Percentage of staff with cyber-related KPIs integrated in their roles (for example, individual performance in phishing drills) Percentage of staff participating in one or more cyber-awareness campaigns in the year (such as a data challenge or cyber-champion campaign) Percentage of staff with access to cyber training adequate for their day-to-day roles
TARGETED BEHAVIOURAL CHANGES 	To measure changes in staff behaviours through objective and quantitative means	<ul style="list-style-type: none"> Percentage of staff who installed security patches only at the point of "forced install" Percentage of critical new threats identified that are not resolved within two days Percentage of staff who completed cyber training within one month of launch
PULSE CHECK 	To measure the organisation's progress in the change being brought about. These metrics measure the mindset shift of the organisation as a whole in the cyber-change programme	<ul style="list-style-type: none"> Employee awareness score on their capabilities to protect the organisation from potential cyberattacks Employee awareness score on organisation's focus on protecting itself, its customers, and staff from potential cyberattacks Employee awareness score on organisation's capabilities to protect itself, its customers, and staff from potential cyberattacks

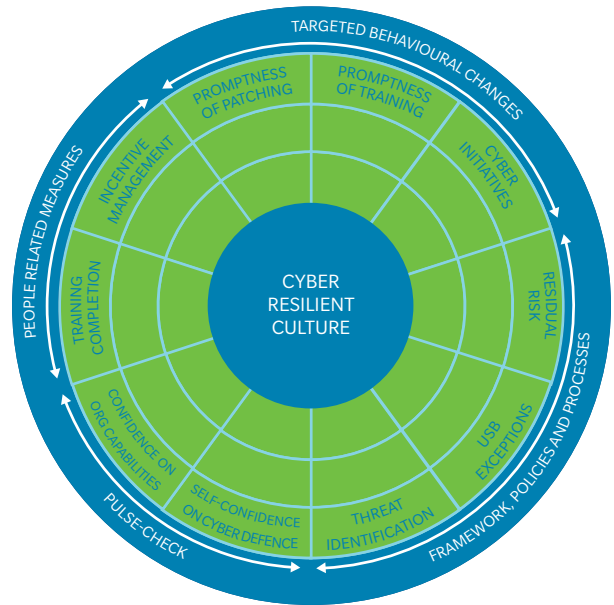
Together, the metrics can be represented in a **cyber-culture wheel**. (See Exhibit 5.) This provides a visual snapshot of the organisation's cyber culture for ongoing monitoring by senior management. Over time, the organisation should aspire to become resilient with respect to different aspects of the culture wheel so as to strengthen its cyber culture even further.

Exhibit 5: Cyber Culture Wheel

CURRENT STATE



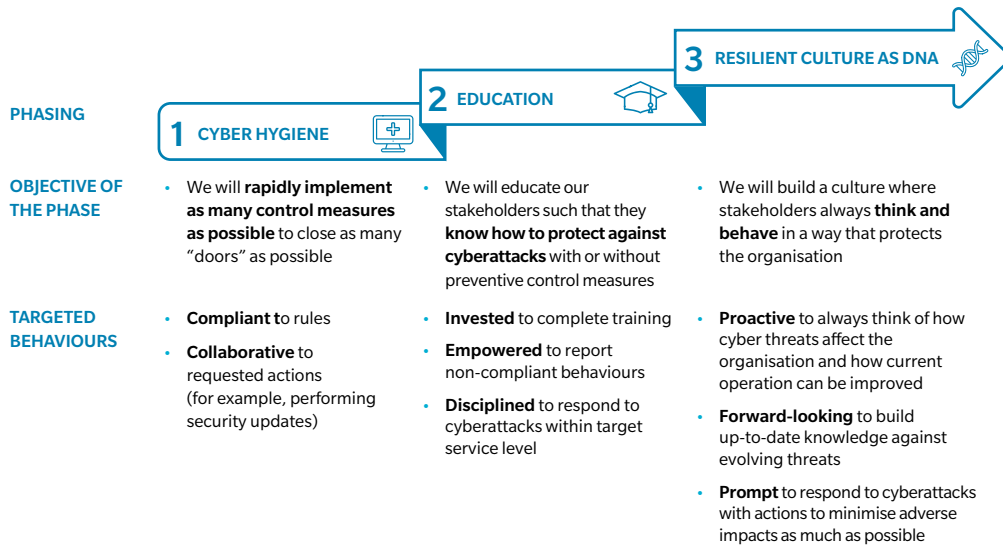
FUTURE STATE



THE RIGHT ROUTE AND PACE TOWARDS CYBER RESILIENCE

Building a cyber-resilient culture needs a long-term effort, not just a one-off initiative. Any change-management programme takes time to change behaviours and strengthen the cyber-risk mindset in the organisation. A gradual and coordinated effort is required to increase the level of cyber-resilience, and it can take between 12 and 18 months to achieve any observable change. (See Exhibit 6.)

Exhibit 6: Behavioural Change Roadmap



As in any cultural change, it is important that organisations follow the right path at the right pace. These will depend on which phase of the cyber roadmap they are at, as shown in Exhibit 6. The path should be supported by relevant **nudges or interventions** to support each phase.

For example:

- **Phase 1:** Initial rapid implementation to close as many doors as possible and enforce compliance. Interventions include measures such as blocking USB sticks, restricting access to the Internet, disabling links in emails originating from outside the organisation, and penalties for employees trying to find ways to bypass these controls (such as using personal hotspots to access blocked websites).
- **Phase 2:** Education for staff to understand the need for cyber-aware operations and how to conduct them. Nudges are typically in the form of rewards for demonstrating good behaviour, such as completing a cyber training programme within two weeks of its launch, reporting phishing emails (and not just deleting them), and reporting other suspicious activities (action-based reviews).
- **Phase 3:** Resilient culture as part of the corporate DNA, as staff become more aware of cyberattacks and their associated perils. Nudges include rewards for promoting cyber-resilience within the organisation through actions such as identification and mitigation of new cyber threats; pro-actively sharing cyber-related news with team members; and peer feedback. Consistent communication over time is important in this phase.

These nudges and interventions need to be carefully designed, as they will only be effective if the details are correct. We recommend that they draw from techniques derived from insights into how professionals learn new behaviours and establish new neural networks. We have found that the most effective tools apply some of the latest thinking from research into neural science, neuro-linguistic programming, and behavioural change. Many of the measures

consist of nudges that influence behaviour on both a conscious level, where many programmes focus, and a subconscious level, where most behavioural change occurs.

In addition to providing models for behaviour, formal and informal communication supports change and uses authority bias and group dynamics to precipitate changes in behavioural habits. In addition to normal corporate change communications, targeted – and at times provocative – communications can be used to help nudge people and get them thinking about changes in their day-to-day working environments.

Ultimately, the goal is for all stakeholders to demonstrate desirable cyber-resilient practices at any time, wherever they are.

A LONG FIGHT FOR EVERYONE IN THE ORGANISATION

Organisations need to realise that building cybersecurity through frameworks and tools is different from building a cyber-resilient culture, which refers to cultivating resilient behaviour in staff. The former might get more headlines and attention today, but one without the other is not sufficient. The resources put into implementing software solutions to build up cyber security must be matched by the creation of a cyber-resilient culture in the organisation. In other words, building cyber-resilience must be treated on a par with building cybersecurity.

An organisation's cyber-resilient culture can be the strongest asset – or biggest vulnerability – in its cyber strategy. It is an ongoing effort towards changing the way staff think and work in their individual roles. It should be driven by investment and attention from senior management and empowered by stakeholders across the organisation. Ultimately, cyber risk is unique in that it deals not with financial ratios, but rather with **evolving threats**. It is therefore a strong illustration of the statement, “**No one can achieve zero risk**”. The journey to building cyber-resilience is therefore a **long-term commitment**. And, as the Chinese saying goes:

“*A journey of a thousand miles begins with a single step*”

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at marketing.mea@oliverwyman.com or by phone at one of the following locations:

ASIA PACIFIC
+65 6510 9700

AMERICAS
+1 212 541 8100

EMEA
+44 20 7W333 8333

AUTHORS

Wolfram Hedrich
Partner
Wolfram.Hedrich@oliverwyman.com

Jayant Raman
Partner
Jayant.Raman@oliverwyman.com

Tanishq Goyal
Engagement Manager
Tanishq.Goyal@oliverwyman.com

Laura Gunarso Novilia
Senior Consultant
lauranovilia.gunarso@oliverwyman.com

Rachel Lam
Research Analyst
rachel.lam@oliverwyman.com

Contributors

Kevan Jones
Partner in OE
kevan.jones@btinternet.com

Lynnette Lin
Principal
lynnette.lin@oliverwyman.com

www.oliverwyman.com

Copyright © 2019 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.

