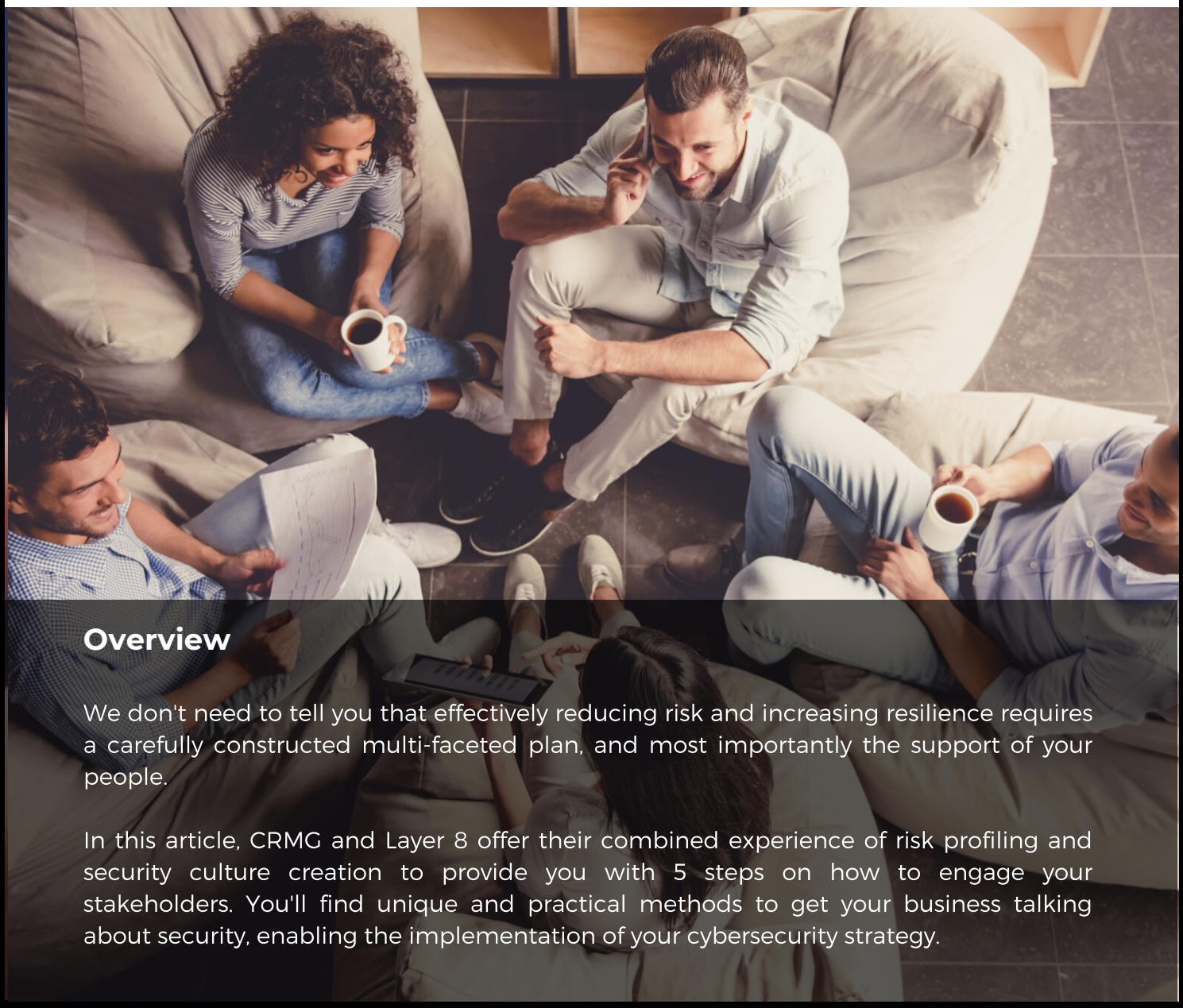
LAYER 8

CRMG
CYBER RISK MANAGEMENT GROUP

Creating Resilience: 5 things cyber-criminals wish your business didn't talk about



Overview

We don't need to tell you that effectively reducing risk and increasing resilience requires a carefully constructed multi-faceted plan, and most importantly the support of your people.

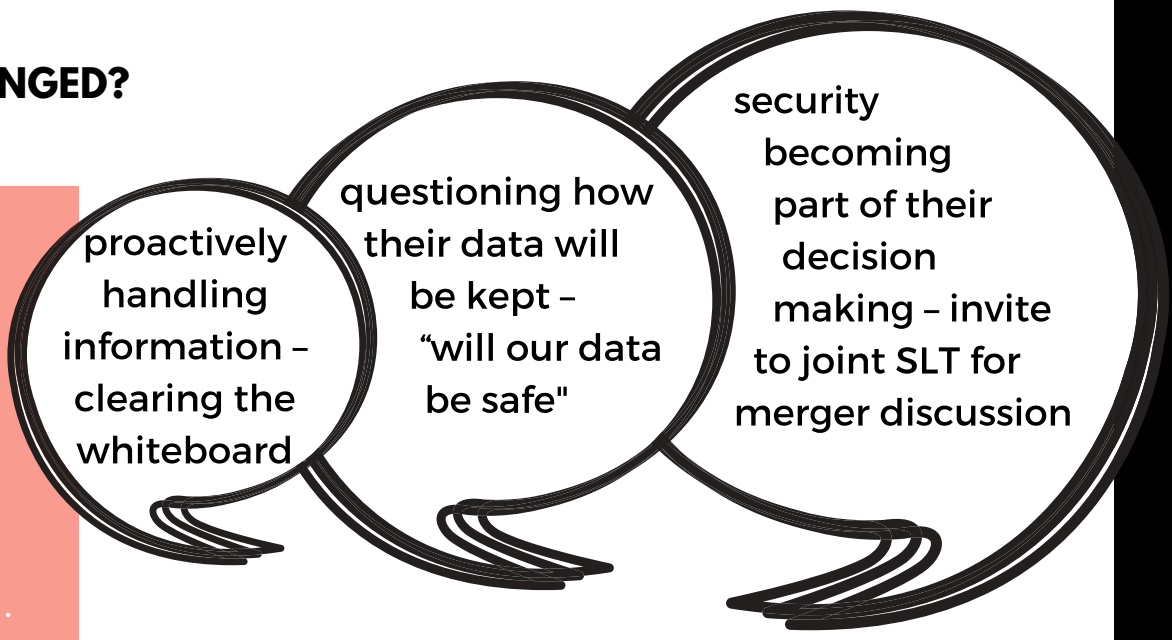
In this article, CRMG and Layer 8 offer their combined experience of risk profiling and security culture creation to provide you with 5 steps on how to engage your stakeholders. You'll find unique and practical methods to get your business talking about security, enabling the implementation of your cybersecurity strategy.

LAYER 8

IMAGINE... you go away for a year. When you return something's changed. You walk into the building on the first day and hear someone ask, "will our data be safe?" You peer into a meeting room and notice the whiteboard being cleared. A member of the SLT approaches inviting you to join them to discuss the cybersecurity implications of a merger.

WHAT'S CHANGED?

CLEAR. EXAMPLES. of CHANGED. BEHAVIOUR.



= a move towards a proactive security culture!

Why is having a proactive cybersecurity culture important?

Because cybersecurity is as much about PEOPLE as it is about technologies and processes, and if your business is TALKING about cybersecurity, it'll be way better positioned to effectively manage risk.

Opening up conversations about cybersecurity is foundational; it means you can:

- develop a cybersecurity strategy suitable for your business.
- spend less time 'fighting' for budget and buy-in.

IT'S ALL ABOUT RISK

RISK DEFINITION	the possibility that we will suffer harm
CULTURE DEFINITION	what we **say** and **do** on a daily basis that demonstrates what's important to us

Therefore, having a poor cybersecurity culture would demonstrate a disregard for security – which is a risk of the highest magnitude in today's 'cyber climate'.

> **TALKING ABOUT CYBERSECURITY IS A 'HABIT' WHERE I WORK**

What we need is for cybersecurity conversations to become habits or norms across the entire business. A habit is something we do regularly and is often hard to give up. Is talking about cybersecurity a habit where you work? You can do a quick self-assessment by following these steps:

1 - find 10 non-security people

2 – do they say 'yes' or 'no' to the following:

- I often talk about security in meetings
- I often talk about security with customers and suppliers
- Security is part of our normal decision-making process
- Security is part of our shared goals
- Security is spoken about by leaders

Why is talking about cybersecurity so important to mitigating risk?

If conversations about (or including) cybersecurity are happening regularly across your business, they can:

- Tell you what people are doing at the grass roots level in the business (not just what the SIEM analytics say.)
- Uncover the priorities of people who are driving the business.
- Establish core strengths that make the exceptional moments possible.
- Improve the outcomes of security plans through collaboration.
- Facilitate the adoption of new behaviours, technology, and strategies.

Conversations enable you to ***implement*** your cyber risk strategy. 'Implement' being the operative word. A strategy informed by many conversations will be different to a strategy you'd create on your own in isolation.

However, implementation of a strategy driven (or at least influenced) by conversations will be simpler. And what's the point in having the plan of the century, if you can't implement it?

WHERE TO START?

Culture is perpetuated by what we hear and see.

Particularly by people who are influential or visible. So yes, a good security culture really does start at the top. But not to forget, cybersecurity is a job for everyone. Gone are the days when security was restricted to the IT function. Your people must understand their responsibilities and it must be embedded in your culture.

'Engage your stakeholders' – you've probably heard the statement a thousand times. But the provision of detailed guidance on how to engage your stakeholders, far fewer!

1. Start with a question

Asking the right question has the power to:

- build rapport
- help you understand what makes people tick, and vice versa
- develop a shared understanding.

Finding the right question is a skill developed with practice. However, use this as a guiding principle for creating a good opening question:

'every question should invite people to tell a story'.

2. Share stories

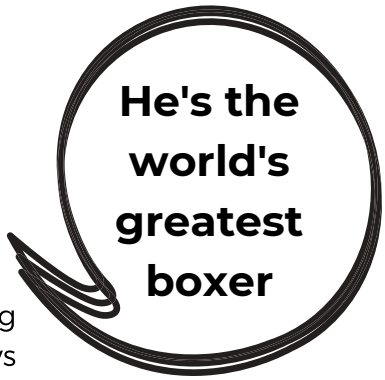
Why stories? When we invite people to tell a story we get more than the well-rehearsed script, what people think they should say or the company line! Inviting a story means people share what makes them tick, what drives them, and how they feel! Stories have power. Power to be shared. Remembered. Replicated.

Our thoughts and feelings matter, because, whether we realise it or not, our focus is driven by our thoughts and feelings, and what we focus on becomes reality. Therefore, choosing to focus on what we do well, will drive change faster than focusing on negatives.

3. Make a choice to focus on the positives

What we focus on becomes reality. For those of us who want to psychologically geek-out then look up 'experience-dependent neuroplasicity'.

Experience-dependent neuroplascticity is about how our brain changes and learns new skills in response to repeated stimuli, cues and learning.



For the rest of us, look up 'Muhammad Ali Trash Talk'. He's the world's greatest boxer. Whether that's fact or perception is irrelevant.

It's not about saying that negatives don't exist. It's about choosing to focus on the positives and repeating the stimuli in various ways until the majority are believing and working towards it becoming a reality.

So in the context of cybersecurity, this means we should roll out the 'cyber fear stories' with extreme caution. Instead, why not focus way more on the role of cybersecurity as an accelerator for strategy delivery?

4. Practice your security trash-talk

So we say this with tongue-in-cheek. But check in with your vocab. If organisations move in the direction they focus, then we want examples of positive security repeated and replicated. Constantly talking about what went wrong is not helpful. It can shift the focus of non-security people away from what they can do to drive improvements.

Make a tally chart. Over the next week put a strike in the relevant box each time you say something, about security, that could be considered positive or negative. Then do the same with the conversations you overhear.

Where does your trash-talk fall? Mostly positive or mostly negative? What new words can you start using to switch the emphasis? How long does it take before you start to hear the new words repeated by your colleagues?

5. Check your basic cybersecurity hygiene

Irrespective of the pace of technical advances, a businesses' information remains core to the creation of a good cybersecurity and governance strategy. Creating a strategy that's right for your business should be based on what you're trying to protect and why. Before you buy the latest bit of kit ask yourself the following questions as a quick baseline assessment:

- Do you know what information your business holds?
- Have you been through a process of valuing business data?
- Do you know what regulations you have to comply with?
- Is there an information security policy in place and accessible?
- Are key suppliers/partners operating to a defined standard?
- Are systems up to date, patched and have anti-malware software installed?
- Are access controls used to restrict access to sensitive data?
- Is sensitive data encrypted?
- Do you backup important business information and has its recovery been tested?
- Do you have a disaster recovery procedure?

The combination of self-assessment of both your basic cyber hygiene AND how you talk about security adds useful introspective context to the risks your business may be exposed to. To turn it into a compelling case the view needs to be widened, incorporating other assessments, evidence and perspectives.

Getting started is about knowing where to focus... not about creating a long list of actions. Your business is unique; therefore, you need to know what will benefit your business most and start there.

EXCLUSIVE MASTERCLASS

On the 7th July at 2pm BST, CRMG and Layer 8 Ltd will be hosting an exclusive masterclass '**From Paper to Practice: Effectively communicating and implementing your cybersecurity strategy**'. We will build upon what was discussed in this paper, providing details, examples and best practices on how to communicate cybersecurity. Most importantly, the masterclass will help you identify where to start with your cybersecurity strategy.

What we will cover:

- Case studies from organisations using this approach and how it has improved their cybersecurity outcomes
- Practical methods to open up conversations with business leaders
- What you need to know about your business before developing a cyber risk strategy
- How to gather knowledge from internal and external sources
- How to prioritise your plan of execution.

REGISTER your attendance here.

ABOUT CRMG

Cyber Risk Management Group (CRMG) is a cybersecurity and information risk consultancy focusing on protecting businesses with pragmatic approaches in line with their true risk profile.

Want to know more about CRMG?

https://www.crmg-consult.com/

@CyberRiskManagementGroup

@ConsultingCrmg

ABOUT LAYER 8

Layer 8 are security behaviour change practitioners with a focus on getting people talking and collaborating about security to reduce risk. Delivering frameworks, training measurement and consultancy.

Want to know more about Layer 8?

https://layer8ltd.co.uk

@Layer8Ltd

@Layer8Ltd