BUILD A SECURITY CULTURE

Kai Roer

EXTRACT

Information Security buzz

itgp™

Build a Security Culture

EXTRACT

KAI ROER

IT Governance Publishing

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

Every possible effort has been made to ensure that the information contained in this book is accurate at the time of going to press, and the publisher and the author cannot accept responsibility for any errors or omissions, however caused. Any opinions expressed in this book are those of the author, not the publisher. Websites identified are for reference only, not endorsement, and any website visits are at the reader's own risk. No responsibility for loss or damage occasioned to any person acting, or refraining from action, as a result of the material in this publication can be accepted by the publisher or the author.

Apart from any fair dealing for the purposes of research or private study, or criticism or review, as permitted under the Copyright, Designs and Patents Act 1988, this publication may only be reproduced, stored or transmitted, in any form, or by any means, with the prior permission in writing of the publisher or, in the case of reprographic reproduction, in accordance with the terms of licences issued by the Copyright Licensing Agency. Enquiries concerning reproduction outside those terms should be sent to the publisher at the following address:

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

EXTRACT

© Kai Roer 2015

The authors have asserted the rights of the author under the Copyright, Designs and Patents Act, 1988, to be identified as the author of this work.

First published in the United Kingdom in 2015
by IT Governance Publishing

ISBN 978-1-84928-716-6

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

ABOUT THE AUTHOR

Kai Roer is a management and security consultant and trainer with extensive international experience from more than 30 countries around the world. He is a guest lecturer at several universities, and the founder of The Roer Group, a European management consulting group focusing on security culture.

Kai has authored a number of books on leadership and cybersecurity, and has been published extensively in print and online, and has appeared on radio, television and featured in printed media. He is a columnist at Help Net Security and is the Cloud Security Alliance Norway Chapter President since 2012.

Kai is a passionate public speaker who engages his audience with his entertaining style and deep topic knowledge of human behaviours, psychology and cybersecurity. He is a Fellow of the National Cybersecurity Institute and runs a blog on information security and culture (roer.com). Kai is the host of Security Culture TV, a monthly video and podcast.

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

FOREWORD

“May you live in interesting times” is an old saying and one that is certainly applicable to cyber security today. As the unfolding events of the past few years have shown us, we are indeed living in interesting cyber times. The evolving cyber breaches of every sector, be it retail, government, education, financial or others, have been the main focus of the technology conversation this entire year. Big box retailers have been hacked, sensitive data at banks breached, and nation states stand ready to wage cyber warfare.

We have developed computers and the Internet and attached many of the most important aspects of our lives to it. Now we find those connections are at risk due to the activities of ‘bad actors’ bent on malicious activity. We try to defend our digital systems with properly configured soft and hardware, but in the end it is often a ‘people’ problem that permits a large portion of the breaches we read about. People are just not following appropriate procedures thereby allowing improper access to systems. As many are aware, the best way to reduce human errors we encounter is through effective education and training. Sadly such education and training around the globe is spotty at best and often wholly inadequate.

With this book, Kai Roer has taken his many years of cyber experience and provided those with a vested interest in cyber security a firm basis on which to build an effective cyber security training programme. This requires change, and understanding how the culture of an

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

organisation needs to change to be effective is vital for cyber success. Each chapter is filled with valuable insights, examples and intuitive thoughts based on his experiences that can easily be transferred to the workplace. As system administrators scramble to harden their respective defences, this work couldn't have come at a better time. Anyone obtaining this book will find it a valuable and informative read.

Dr. Jane LeClair
Chief Operating Officer
National Cybersecurity Institute, Washington, D.C.

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

CONTENTS

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

INTRODUCTION

Culture: Does it have to be so hard?

In this book, I look at organisational culture with information security glasses. In my years of working in the information security industry, I have come across a number of challenges: technical, compliance, and increasingly awareness and security behaviour. Through my travels and company activities, I have learned that a lot of security behaviour challenges are universal: preparing information security information in such a way that it resonates and makes sense for non-security people is a challenge no matter which country or organisation you work in.

I have also learned that some organisations are better at creating the security behaviour they want. Looking at what they do differently, I found that they approach the work with security awareness as a process. They also respect that security competence is exactly that – a competence that must be learned, not just something you tell.

From more than two decades of professional training and consulting in more than 30 different countries, I have also come to learn that if we want people to learn, we need to facilitate learning together with them. Lecturing alone is not creating results. Reading alone makes for very little change. The saying of the Association for Talent Development (ATD[1]) that "Telling ain't Training" is very true. It took me some time to realise that I too had to learn

[1] Formerly the American Society for Training and Development (ASTD).

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

how to train people properly, a realisation that took me on a rollercoaster of learning, exploration and self-development, leading me to develop my training and communication skills across both language barriers and cultural barriers.

The most important thing I learned in these years was to be humble. Humble about my own perspectives – I may think I am right, and I may have all the experience to tell me I am right, but implant me in Tunisia or Japan and most of my perspectives and experience in treating and communicating with people no longer hold. I learned this the hard way, leading me to realise that there are more ways of doing things than I first accounted for, and that others may achieve great success by choosing a different path than the one I chose.

The same is true with organisational culture. There are many ways of building, changing and maintaining organisational culture. It is one of those areas where scientists and practitioners still argue about the right approach[2]. My experience is that the right approach depends on each case. Every organisation is unique and comes with its own culture and subcultures. Some are great, some really poor. All of them impact the behaviour, ideas and thoughts of the employees. The question becomes: how do we take control of that culture?

EXTRACT

[2] A quick search through academic papers via Google will amply demonstrate the variety of approaches within academia alone, while a similar review of the titles available on Amazon reveals a similar breadth among practitioners. For a comprehensive review of the topic (and many other topics!), read Bernard Bass' *The Bass Handbook of Leadership: Theory, Research, and Managerial Applications*.

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

As luck has it, there are processes and methods to apply when you want to build and manage culture. Instead of trying to come up with everything yourself, you can learn from frameworks like the Security Culture Framework[3]. Using a framework gives you a clear path with checkpoints and actions that ensure your efforts are moving in the right direction. This is not to say that changing culture is easy, nor fast: it may require many small steps iterated over time. Using a structured approach helps you to do the right things at the right time, making success more likely.

The book consists of eight chapters, each looking at a different aspect of security culture. Chapter one introduces the concept of security culture, provides a definition and sets the stage. In chapter two, I look at the three building bricks of culture: technology, policy and people. I also bind the three together and show how they impact one another.

In chapter three, I look at how security culture relates to security awareness, and I will show how awareness is only one of the elements that is required to change behaviour and culture. Next, in chapter four, I explain why we as security professionals are not the people who should build culture – at least not alone – and who you should involve in your organisation. In chapter five, I point to social psychology and research on how we interact with other people. You will also learn how you can use the knowledge of how groups impact our lives to increase your chances of improving security culture.

[3] The Security Culture Framework describes a structured approach to developing an effective and consistent security culture within an organisation. Read more about it here: *https://scf.roer.com*.

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

In chapter six, I make the case for why we need to measure our security culture efforts, and point to some ways to do just that. Finally, in *chapter 7*, I introduce the Security Culture Framework, and walk you through how it is built. This chapter also includes some templates you can use in your own security culture programmes.

Depending on your perspective, I may provide new insights and ideas on how to build security culture. I hope I can inspire you to take a structured approach to building and maintaining good security culture. Even if you do choose a structured approach, you will experience that it takes time to get the results you want. Small steps, iterated over time, is the key. Knowing where you are, and where you want to be, is vital, and one of the key elements in a structured approach.

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

CHAPTER 1: WHAT IS SECURITY CULTURE?

An introduction to the topic, with an introduction to the definition of culture (based on sociology) and how it relates to security.

Humans are animals who live in groups; we flock. In any group of animals there exists a hierarchy, levels that every animal in the group follows. Each of these levels comes with rules to abide by, including understanding who is above you, who is below you and what your particular level allows you to do.

Consider a wolf pack[4]. They show the hierarchy very clearly, with the Alpha couple on the top, giving them the right to rule as they please. Below them are sergeants, animals in the pack with more power than most and which police the group if necessary. Below the sergeants are normal members, workers if you like, and below these again are one or a few of lesser rights – the one or two wolves that are constantly being picked on. Every animal in the pack has the right to food, shelter, safety and protection – as long as they abide by the rules and accept their level. A wolf on the lower levels will quickly and

[4] It should be noted that the traditional view of a wolf pack as led by an Alpha and his mate is a grand simplification, and many biologists prefer to refer to 'breeder wolves' (note the plural) as the centre of the pack. This does not undermine my point here, however, as the broader structure of the pack as a unit offering its members protection and belonging in exchange for acceptance of the rules and hierarchy is undoubted.

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

effectively be controlled by the other wolves if he or she dares to step out of line.

Even the poorest wolf in the pack is entitled to the pack's protection against external threat. They are also entitled to love and care, even if they are expected to give more than they receive.

The wolves in the pack accept the hierarchy, rules and domestic violence because they receive protection from external threat, they get to eat and they may even enjoy the sense of belonging. It makes sense for the wolves to stick together, even if the price an individual wolf pays is a certain loss of personal freedom.

We see similar tendencies and mechanisms play out in human society. The first rule of living in a society is to accept the rules. To do that, we also need to understand the rules, how they are constituted and how they are playing out.

Consider the wolf pack again. Let us imagine a new wolf is in the pack (it could be a puppy becoming an adult, or adoption, or anything else). This new wolf is entering the pack at the second-to-lowest level, so he is accepted as a worker, someone with little status. However, this particular wolf cannot understand the rules at play, and imagines himself as the leader of the pack. At first, the other wolves just mock him a bit, to remind him of his place. Then, when he clearly does not get the message, they become more violent, with the Alphas and their sergeants leading the punishment. The violence continues until the wolf rolls over on his back and surrenders. He gets the message, he understands that there is someone else above him in the chain of command, and that if he wants to survive and be a part of the pack, he must accept his role, his place.

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

Just like the wolf, we need a basic understanding of authority if we want to succeed in life.

Thankfully, luck is with us. According to some scientists, the human brain is hardwired to understand the power structure of the people in a room[5], and to automatically identify with our own level. This particular science is based on babies, too young to communicate verbally, who still recognise the power levels and authorities in a room.

Why does this matter to us? This kind of research suggests that the need for policies, rules and laws is part of the basic functioning of the human mind. It suggests that although the way we currently organise our societies can be considered social constructs, we humans (social animals) come pre-programmed with the ability to form, abide by and live in groups based on different levels and authorities.

It basically tells us that our ability to live together in small and large groups is a biologically developed ability. We are meant to form groups and find ways of living together.

This is an important backdrop to understanding what culture is. According to the Oxford English Dictionary, culture is:

> "The ideas, customs and social behaviours of a particular people or group."[6]

EXTRACT

[5] In the study "Big and Mighty: Preverbal Infants Mentally Represent Social Dominance" (L. Thomsen, W.E. Frankenhuis, M. Ingold-Smith and S. Carey), it was found that babies expect larger individuals to win in a conflict. For a baby to make that prediction, they must have some comprehension that individuals have goals, and that these goals can conflict with other individuals' goals. Furthermore, they must understand that these conflicts have winners and losers.

[6] There are a number of different definitions of culture, including security culture. I have chosen the ones I use in this book based on the premise that they

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

Part of the behaviours we see in culture can be traced back to basic human biology as I showed earlier. It is good to know that culture is such a base need in us, as it shows the importance of living, working and functioning together.

Most of culture may not be so basic, and it is certainly not traced to biology alone. Most culture is learned[7]. One of my favourite examples is how people walk. “How can the way people walk be culture?” you may ask.

That is a fair question, considering that we all walk the same way. We all put one foot in front of the other. So far, I agree.

What is different is *how* we put one foot in front of the other.

In the western world, where I grew up and lived most of my life, we wear shoes. Mostly comfortable shoes, enabling us to thump our heels onto the ground without being hurt (at least not right away). We also wear high heels, which is not exactly a natural way of walking, even if walking on your toe-balls and mid-foot is considered the natural way of walking.

EXTRACT

describe what I discuss in layman's terms, which makes it accessible for people outside of academia.

[7] This is also debated – behaviorists take this stand, while naturalists believe behavior (and thus culture) to be inherited, more similarly to genetic inheritance. The truth is likely somewhere between those extremes. Richerson and Boyd describe the naturalists' position: “Cultural variants are more like genes than are ordinary learned variants. Like genes, they are inherited and transmitted in a potentially endless chain, while variants acquired by individual learning are lost with the death of the learner.” (“Cultural Inheritence and Evolutionary Ecology”, *Evolutionary Ecology and Human Behaviour*, 1992.)

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

Unconvinced? Come with me to Africa, then. Here, many people walk barefoot, which means they walk differently from you. Go to Kenya, where some tribes run because they consider walking a waste of their time. Am I getting there? Not yet? Well, my last example is from Asia.

In Japan, traditional shoes are made of a plank, with two wooden pieces underneath. Walking with these shoes dictates a particular walking style – instead of lifting your feet, you slide them along the ground, sort of.

Still not following me? Wear high heels one day, and I promise you will get the idea. How we walk is learned behaviour. A behaviour dictated by the culture we live in. Your ability to recognise what I mean by my claim about walking, is cultural: it is a learned behaviour. It depends mostly on your exposure to different cultures, different people and different places.

The definition of culture is the same: *ideas, customs and social behaviour of a particular people or group*

As we have seen in the preceding example, ideas, customs and social behaviour are collections of many things – from how we walk, to how we speak, to how we think and interact. Instead of thinking about culture across borders, let us look closer to where we work. Consider your workplace. Culture is not one thing only; it is the accumulation of many groups of people: the sales department, the accounting department, the IT department, the developers, the builders, testers and so on. Each of these departments has its own more or less distinct culture – ideas, customs and social behaviours that belong to that particular department. Together, these *subcultures* form the company culture. And some of these

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

departments are also subdivided into other subcultures: smokers, the high achievers, the slackers, the coffee drinkers, the problem solvers and so on (I am sure you can think of others more fitting to your organisation).

You, as an individual, are a member of many different groups, and more or less abide by each group's cultural rules. In your workplace, you may be working as a mid-level manager, drinking coffee, placed in the IT division and be a high achiever. Each of these groups comes with a cultural attachment.

Outside your workspace, you also belong to different groups, each with different characteristics: your family, your extended family, perhaps you are a parent, you may be playing sports (each team/group you belong to has different subcultures), you are a community member and so on.

Each of the groups you belong to follows the same basic principles. They consist of People: the members; Policies: the rules this particular group follow, sometimes written and always the unwritten ones; and Technology: the tools, methods and models used by this group. You can read more about these three elements, and how they come together to form and change culture, in *Chapter Two*.

Now that we have a quick introduction to culture, let us examine it from a security perspective.

According to the Oxford dictionary, security can be defined as:

> "The state of being free from danger or threat."

Using this definition helps us understand what we as security professionals do: our job is to create an

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

environment where our colleagues can work in a *state of being free from danger and threat;* they can do what they are supposed to, knowing that they will be taken good care of, that external threats and dangers are being kept outside.

In the image of the wolf pack, this becomes very clear: as a member of the pack, each of the wolves are entitled to food, to protection from external threat and to know their place. They get *security* by living in the pack. The same strategy is used by a number of different creatures, and has proved very successful.

One way of being free from danger is to know the social structure, and your own place in it. Understanding where you are in the organisation, and what is expected of you is crucial to properly functioning in a group. This is one of the reasons it is important to communicate clearly, and to express the security behaviour you want in your organisation in a way that employees can relate to.

EXTRACT

Since culture and social behaviour is so engraved in us by nature, it makes perfect sense to understand how to use nature's own strategies to enhance security in our organisations. Enter Security Culture.

Think of security culture as one subculture of your organisation's culture. The security culture is the part of your organisation's culture that focuses on security, *to help people into the state of being free from threat or danger*, and you can apply the same techniques used by organisational theorists, transformational theory, sociology and psychology to understand and enhance your organisation's security culture.

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

Using the two preceding definitions, we can define security culture as

> "The ideas, customs and social behaviours of a particular people or group that helps them be free from threat and danger."

Security culture is the ideas, customs and social behaviour that your organisation, and its subgroups, have, use and act upon to create a state of being free from threat and danger.

The way your organisation treats passwords is part of security culture. How your employees detect and act upon a stranger in the building is part of security culture. How you define policies, implement them and train employees in security behaviour all impact your security culture.

In fact, all the social behaviours in your organisation impact your security culture. Security culture also impacts all social behaviour in your organisation: it becomes a question of who is in charge of the social behaviour, You or the Culture.

Sometimes I hear that changing culture is impossible, or at least very hard to do. As with security awareness, who some find very hard to teach successfully, cultural change is possible. It is, in fact, a given. Culture is, according to sociology, plastic[8]. It adapts to its members.

Think of it like this: without a group of people, there would be no culture. Culture demands at least two people.

[8] The other characteristics of culture are generally given in the following statements: culture is learned and acquired; culture is shared and transmitted; culture is social; culture is ideational; culture gratifies human needs; culture tends towards integration; and culture is cumulative. (E. Palispis, *Introduction to Sociology and Anthropology*, 2007.)

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

These two people, together, form the ideas, customs and social behaviour of this particular group, by their actions and activities. The culture is likely highly influenced by the larger culture that formed the two members in the first place – including language, social belief and so on. Even so, the group will form a distinct subculture, with its own rules, ideas and customs.

Then, some time later, the group welcomes a third member. This new member brings her own ideas, customs and social behaviours. Let us say that the group's initial members met at a pub and drank beer once a week. The new member meets them too, but starts drinking wine instead. Just by drinking wine instead of beer, the culture of the group has changed: it can no longer say "we drink only beer." We may even imagine that six months later, the whole group moved from the pub to a restaurant and they are all drinking wine while enjoying fine dining. The group is the same three members, but the culture has changed a lot!

EXTRACT

This example shows how quickly, and easily, culture can change if the majority of the members, or the ones with the right authority, set out to do so. It also shows that culture can change *regardless* of original intent. In this particular group, a stranger created enough impact to change the whole group culture.

Another example is the coffee-machine example where someone begins working at a new employer. The new employee is a coffee drinker, and quickly figures out where the coffee machine is. As soon as she knows where it is, she only takes a few days to adapt her behaviour to the coffee culture at the location, no matter how they do their coffee-machine ritual.

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

This example shows how quickly we as individuals adopt a new culture when we are correctly *incentivised*[9].

The impact of individuals in a group is very important. Think of a group of people, say a team at work. This group has no strong culture, and are a loosely knit team of people working together. Without a strong culture, a group like this is more vulnerable to outside pressure, and to uncontrolled cultural change.

Into this group comes a new team member. This person is very negative. He sees problems everywhere, and is a specialist in killing enthusiasm. Suggesting an idea to this guy is a sure-fire way to be shot down, publicly humiliated and buried under a pile of sarcastic rocks. And no, it does not matter who approaches him with suggestions, ideas and opportunities: he immediately says things like, “No, it’s never gonna happen” or “I saw this before, it failed.” On particularly bad days, he may even say “Are you stupid, or what?”

EXTRACT

What happens to a group when such a person is introduced? It depends on the group’s culture. A group with a strong culture is more likely to change the newcomer into conforming with the culture (or force him out), whereas a group with no strong culture is more likely formed by the new member. In this case, since the group has no strong culture, they quickly become a gang of grumps. Their production rate deteriorates, and their

[9] According to motivational theory, there are two broad forms of incentive: intrinsic and extrinsic. An intrinsic incentive is derived internally – the individual is motivated to perform because they enjoy the work or the challenge, for instance. An extrinsic motivation is applied from without – the employer offers a cash bonus if the employee completes a task quickly, for instance. It should be noted that there are negative forms of both types of incentive, such as the threat of being fired, etc.

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

problem solving is replaced with problem focus: instead of finding solutions, they only see problems. The group adopts the newcomer’s attitude.

In this example, a productive and functioning team was destroyed by just one person. Imagine the cost for the organisation that this cultural change has. Then consider the personal and interpersonal costs involved in this cultural change: people in the group are no longer happy to go to work, and they may even change their social behaviour towards their friends and families!

That is the kind of impact culture has on people, and the impact people have on culture. Since I *choose* to be a positive force wherever I go, I will end this chapter on a positive note.

EXTRACT

Consider the same group as before, a team of people working together. There is no strong culture in the group, and their social behaviours, as before, are neutral and flexible. This time, the team member we introduce is a positive person, one who sees opportunities where others see problems, and one who helps people succeed instead of killing every idea.

Since the culture in the group is neutral, our new group member can easily change it, just like we saw with the negative example before. Just like the negative influencer, positivity is contagious too. At first, one or two of the other team members will enforce their positive traits, and after some time, the positivity spreads throughout the whole team.

Other teams in the organisation will notice too, and may want to join the team – after all, who does not want to be a part of a success?

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

These examples show us how culture can be a vulnerability to your organisation too. When it comes to changing culture, going from a neutral, weak culture is easy. To change a strong culture may not be so simple. Understanding the cultural impact on your organisation, and to your security programme, is vital if you want to create a human stronghold to fence off external threat.

In the next chapter we will look at the building blocks of human culture: People/Competence, Policies and Technology.

EXTRACT

Case Study: Introducing John, chief information security officer

A case for Culture

John is a chief information security officer (CISO) in a large bank. He is, as most CISOs are, a very busy man, juggling strategic planning with tactic reporting, and trying to make his team of three do every task they need to, while also securing budgets to improve security around the bank.

For a long time, John has tried to train the employees on awareness. To ensure compliance, he runs security awareness training for all new hires, a part of the bank's employee on-boarding programme. He also has at least one awareness training campaign running throughout the bank every year. In his reports to the directors, he states that 95% of new hires have

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

successfully completed the on-boarding training programme, and he also reports an 87% open rate and a 64% completion rate of the annual awareness programme.

John is not confident that his reports are meaningful, and he is not sure if the numbers are showing the bank's actual awareness level. In fact, John is uncertain if his ongoing efforts are creating any results at all, as successful phishing attempts have risen during the past 12 months, and a steadily growing number of password reset requests is a concern. In addition, he has a hard time motivating any of his team members to do any awareness work at all, even when he gives them direct orders.

In a recent board meeting, where he presented his numbers on awareness, Jillian, one of the directors, asked him if the numbers meant that the bank was in a secure state, and she also wanted to know how their bank compares to other banks in the industry.

Puzzled by Jillian's questions, he said he was confident in his numbers, and that as far as he knew they were doing ok. Only after the meeting did he realise that he did not really know. He decided to look into the matter.

Over the next month, John spent his time researching. What he found was alarming. The more he looked at his numbers, the more he realised they were vanity metrics – a term coined by Eric Ries in his book *The Lean Startup*, a book John was told by one of his friends to read. Vanity metrics are numbers that looks

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

good, and seemingly provide value, but in reality do not provide any answers. John realised that his reports for the past few years did not give him or his bank any real measurement of their progress, nor the reality of their security culture and behaviours.

He also realised there were very few benchmarks on security awareness, and that he had no clue whether or not his bank was as good as the others.

As part of his research, John also stumbled upon the Security Culture Framework. He approached me, and together we created a three-year plan to change the approach of his security awareness efforts: we created a plan to build security culture. We devised a plan for John to create a metric that allowed him to understand his landscape. We also defined a series of goals, which he described in a way that ensured he would know when he hit, or by how far he missed, his targets.

Another challenge that surfaced in our talks was the lack of strategic cooperation between the security team and the rest of the organisation. John and his team would do their configurations, implement policies, put out fires and so on, and most of their communications with other departments were perceived by the organisation as being negative. Many saw John and his team as naysayers. Using the organisation module, John learned to adapt a few strategic communication tools, and to build rapport with people and managers around the bank. I also urged him to build a deep and meaningful relationship with Human Resources.

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

Finally, John needed a way to handle his team's negativity towards awareness work. When asked, a team member would reluctantly accept an awareness-related task, but it was very clear that none of the team members found that kind of work interesting. John had to tackle this challenge, and quickly!

Throughout this book we will follow John as he endeavours to build security culture, by digging into each of the preceding cases.

<<< END OF EXTRACT >>>

EXTRACT

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

Build A Security Culture

- Understand how to create a culture that promotes cyber security within the workplace.
- Using his own experiences, the author highlights the underlying cause for many successful and easily preventable attacks.

"With this book, Kai Roer has taken his many years of cyber experience and provided those with a vested interest in cyber security a firm basis on which to build an effective cyber security training programme."
Dr. Jane LeClair Chief Operating Officer National Cybersecurity Institute, Washington, D.C.

Buy your copy today

www.itgovernance.co.uk/shop/p-1687-build-a-security-culture.aspx

www.itgovernanceusa.com/shop/p-1463-build-a-security-culture.aspx

www.itgovernance.eu/p-1113-build-a-security-culture.aspx

This extract and the original text it is taken from are both subject to ITG copyright and may not be reproduced, in any form, without prior written consent from the publisher.

EXTRACT