How to build and maintain security culture in any organization.

In this presentation, you will learn about the building blocks of security culture, and how to organize your security culture program to create success.

Slide 2

Security Culture Eats Strategy for Breakfast!

Why should we care about culture, you may ask. In leadership, here represented by Petter Stordalen, the Choice hotel chain owner, the realization that *culture eats strategy for breakfast* is the understanding that you can have the best of plans and the best of execution, but without an organizational structure and a common set of values, you will fail. Culture is the building blocks of society.

Slide 3

What is security culture?

Security Culture – what are we talking about? Is this just another one of those marketing tricks? Another fancy name? Let us examine what security culture is. To do that, we need to understand what culture is.

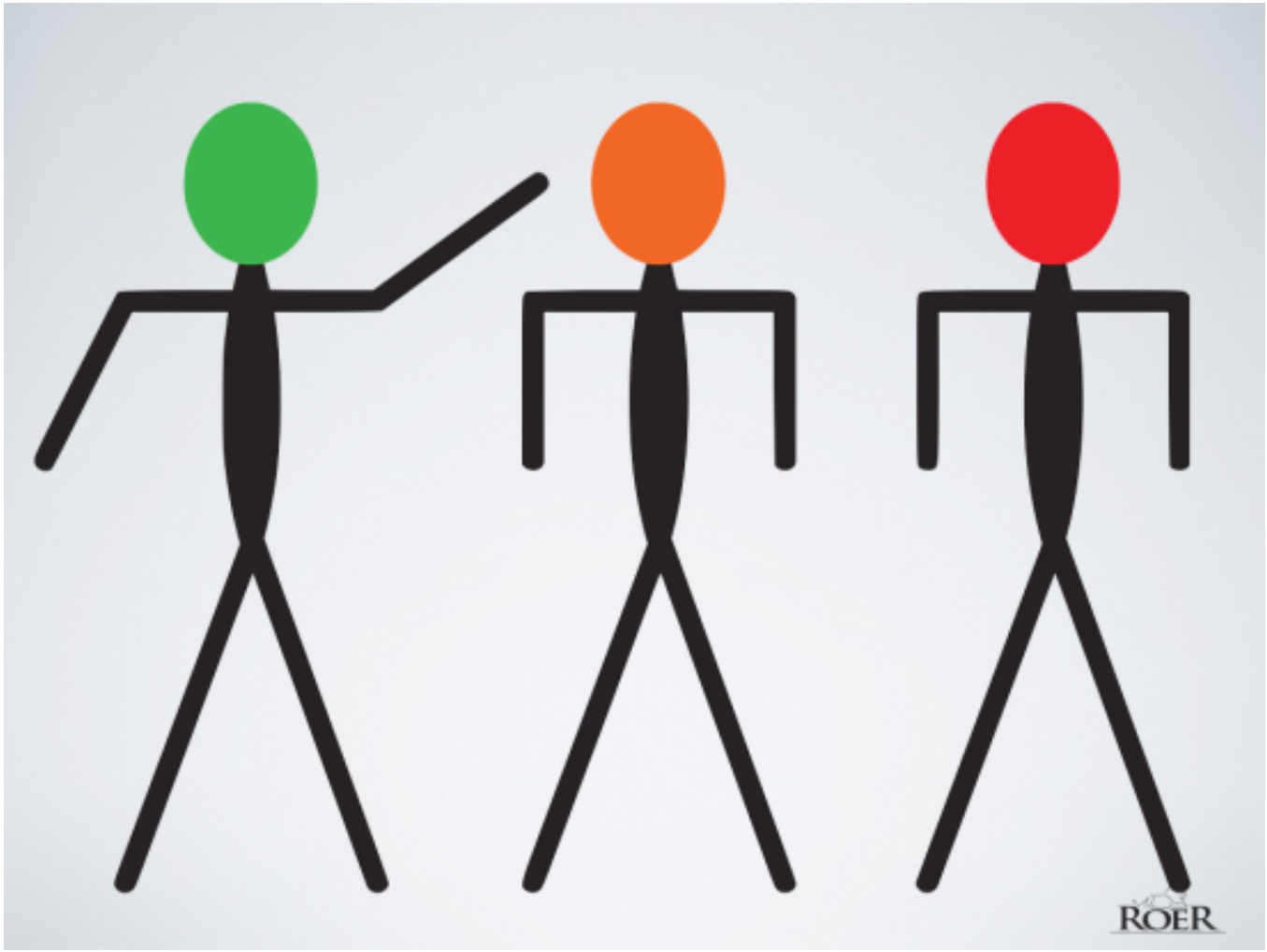
Slide 4

Definition of Culture

The Oxford Dictionary defines culture as: *The ideas, customs and social behavior of a particular people or society*.

Take a moment and think about that. Ideas. Customs. Social behavior. Those are common things every individual shares. You have them – and I do too! And when we meet, we form groups that end up sharing some or all of those ideas, customs and social behaviors. Let us examine culture a little more!

Slide 5



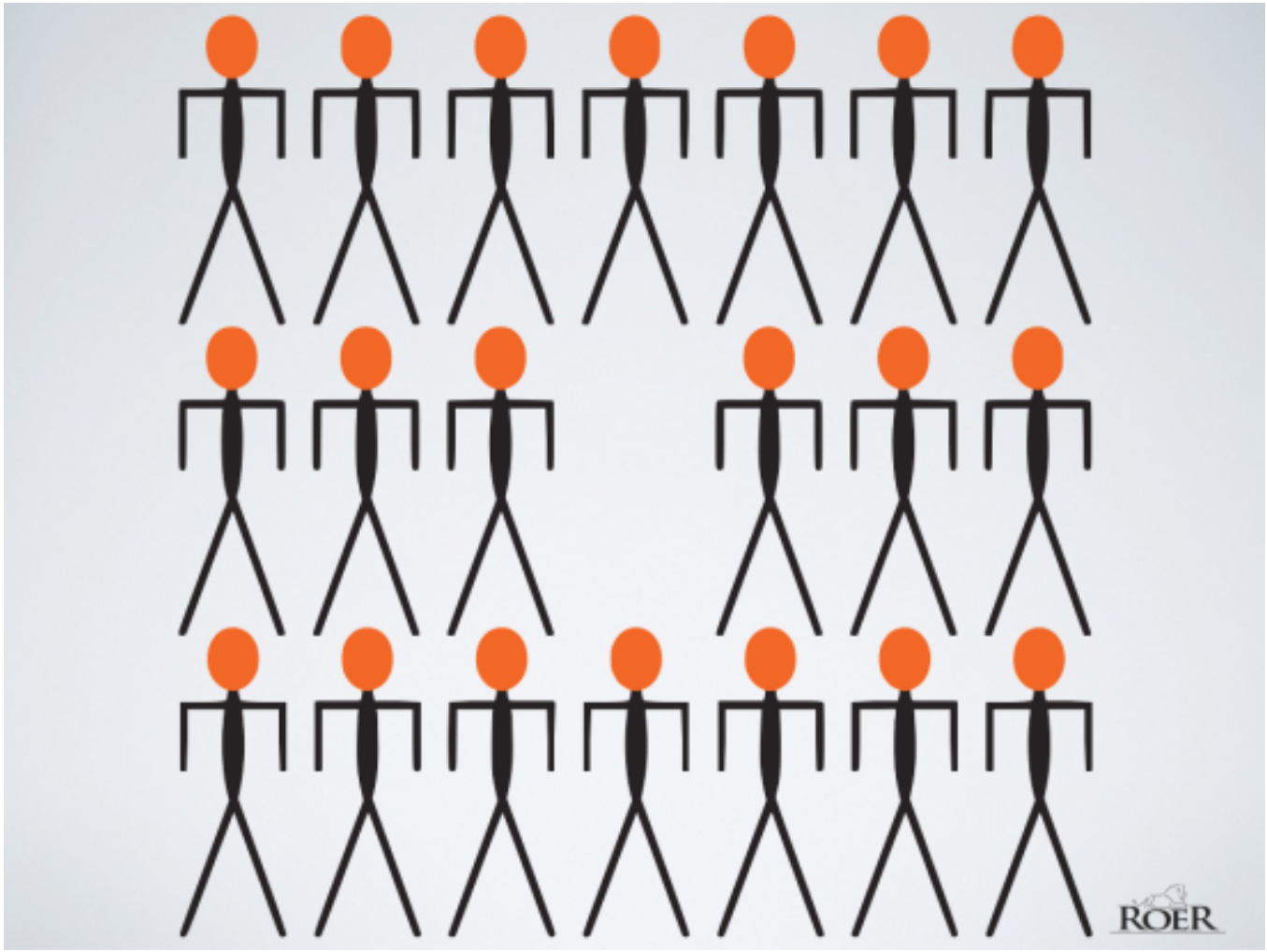
Meet Red, Orange and Green!

Meet Green, Orange and Red. These are individuals as you can see, and they come with their own ideas, customs and behaviors – you can see Green is the positive, including guy, and Red is, well, on the other end of the scale.

We all know these people, don´t we?

Which one are you?

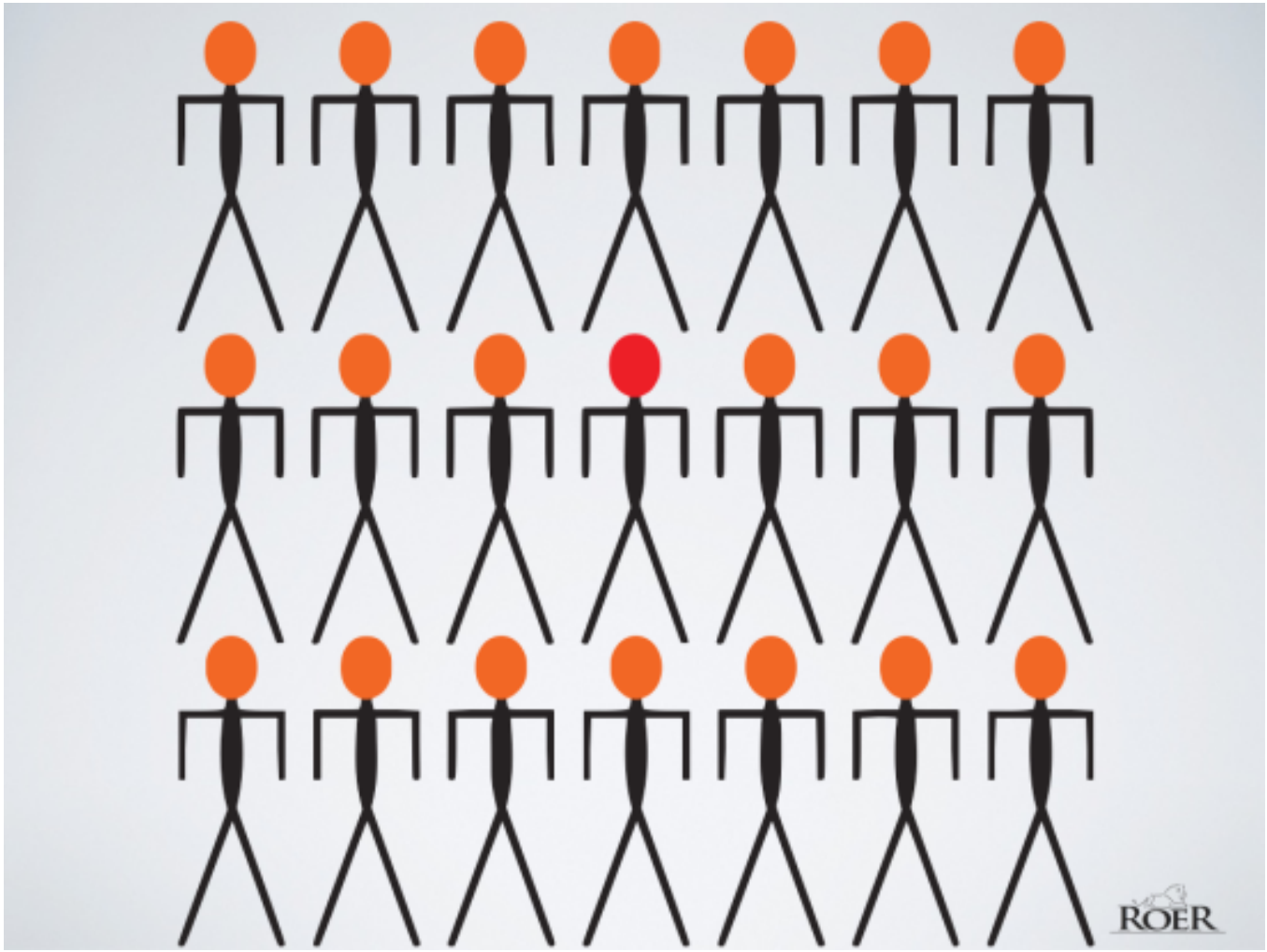
Slide 6



A group of Orange people, forming Orange culture.

Here we have a group of people – they share the Orange values, they form a culture. This could be your work-group, your organization, your soccer team and even your country! They are all examples of groups of people, who together share a set of ideas, customs and social behaviors. In Norway, for example, we share the custom of enjoying Brown Cheese (brunost), which as far as I know, no other country does.

Slide 7



Orange meet Red.

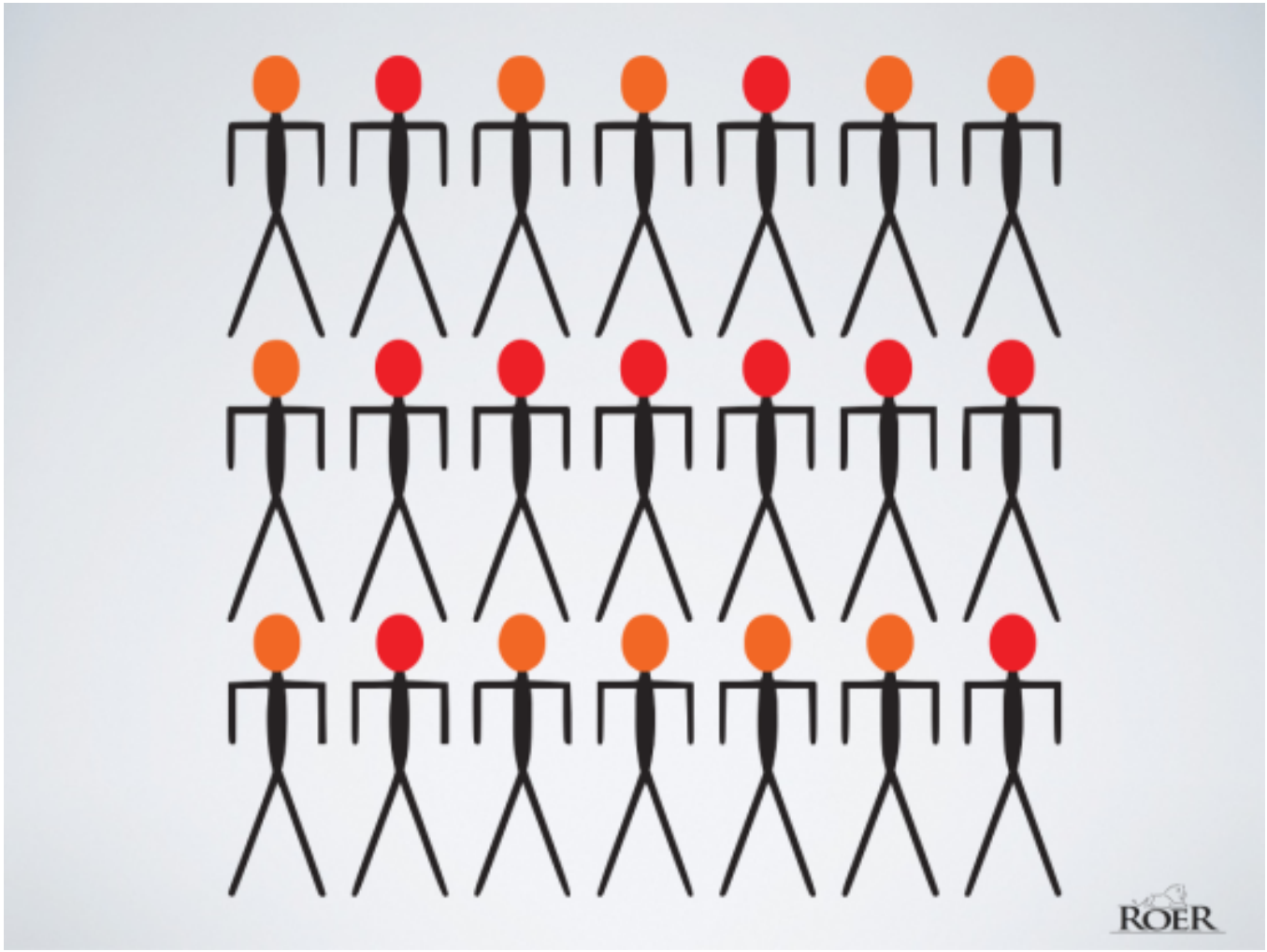
Now, let us introduce Red to this group. Red is, as we remember, the negative person who always gets in your way, looking for the worst, expecting a disaster in every project. The question becomes – will the group change Red? Or will Red change the group? Both are valid questions, and valid outcomes.

Slide 8

Spreading Red.

In the Orange group, however, we do not have a strong culture, which allows a stronger influence from one individual towards the group. And we see the Red ideas, customs and social behavior spread.

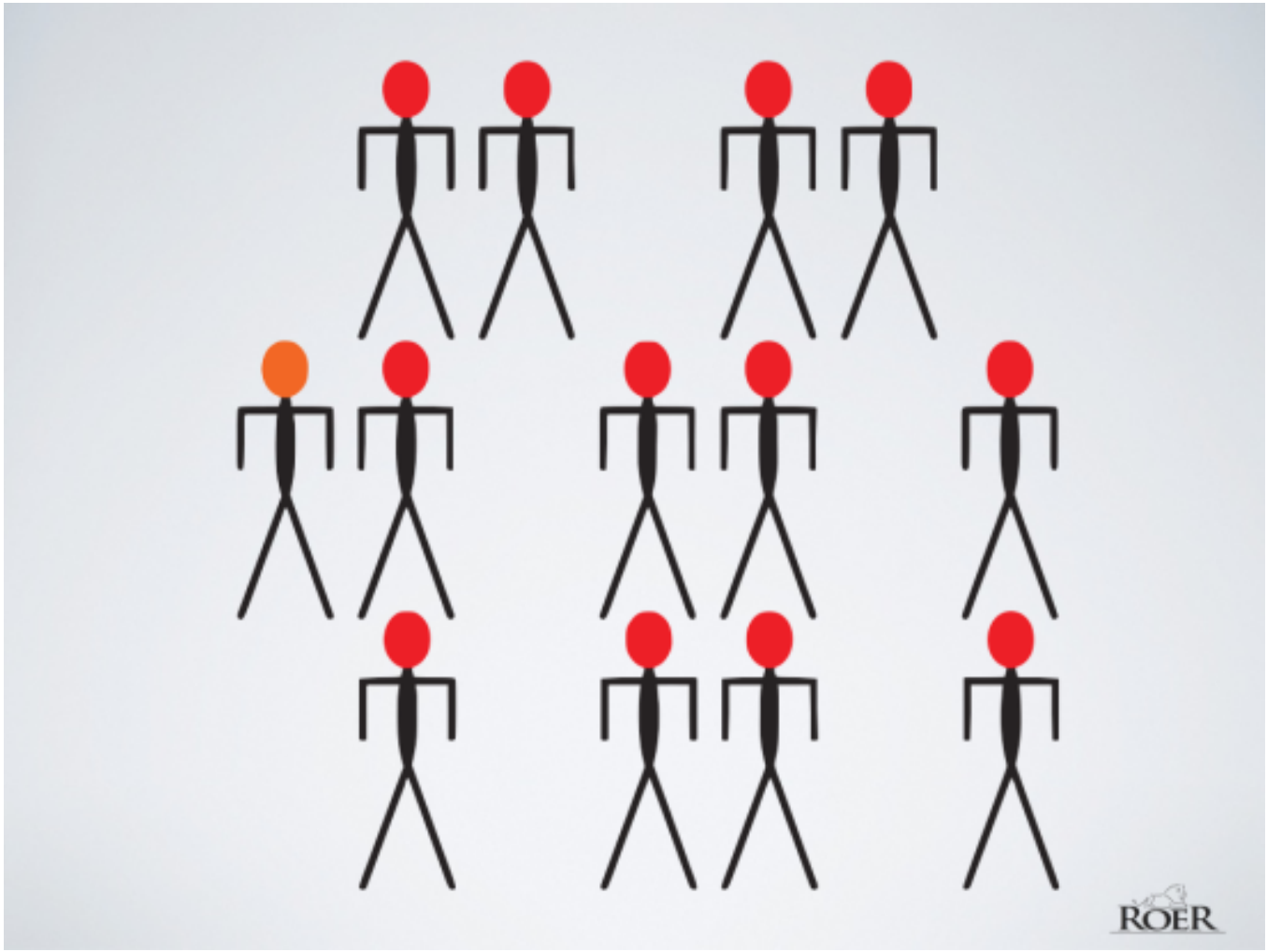
Slide 9



Red culture conquer the Orange.

As we see here, Red is changing the group, by spreading the negativity, the pessimistic outlook. All that is needed is a group who is not focusing on building a strong culture to support itself. When someone new arrives, they are able to change the ideas, customs and social behavior of said group, and can create devastating results.

Slide 10



The devastating results of bad culture, creating fragmentation and negativity.

A result where other members of the group no longer want to be a part, and start leaving. What is left of your team, your department or your organization, is the negativity, the pessimistic outlook and the general consensus that nothing is possible, nothing can (or will) ever change. What is worse, is that this new culture will scare away possibly great additions to the team – or they will leave after only a very short time with the company.

Why should you care as a security officer, you may be wondering?

Remember the Insider Threat, so famously named because it is someone from within your organization who leaks your data, or who introduces malware? An organization, department or team with this negative culture is more likely to create an environment where the insider *willingly* starts exploiting the organization. And that, my friend, that is your problem!

Slide 11

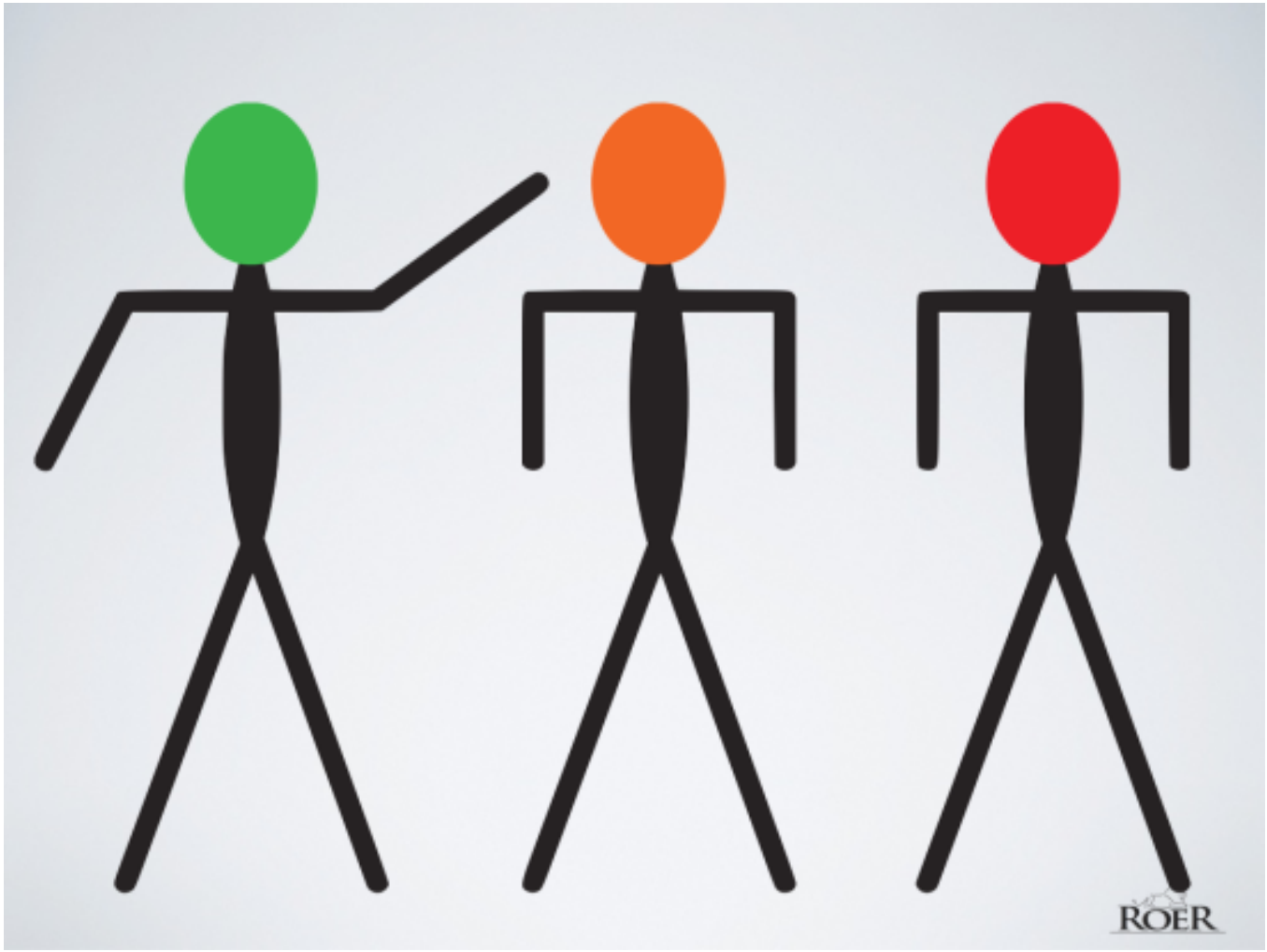
Defining Security.

Let us take a look at the definition of security, again according to the Oxford dict. Being secure, is *the state of being free from danger or threat* and/or *the state of feeling safe, stable, and free from fear or anxiety*

Using this definition, we can see how culture and security walks hand in hand – it is about individuals, people, and groups of people, and it is about creating an environment where people can be free from danger or threat, and where they can feel safe, stable and free from anxiety.

So I claim that your job is to make your colleagues feel safe, and free from fear – which means we should ditch FUD right away! It also mean you may have to reconsider how you do your job.

Slide 12

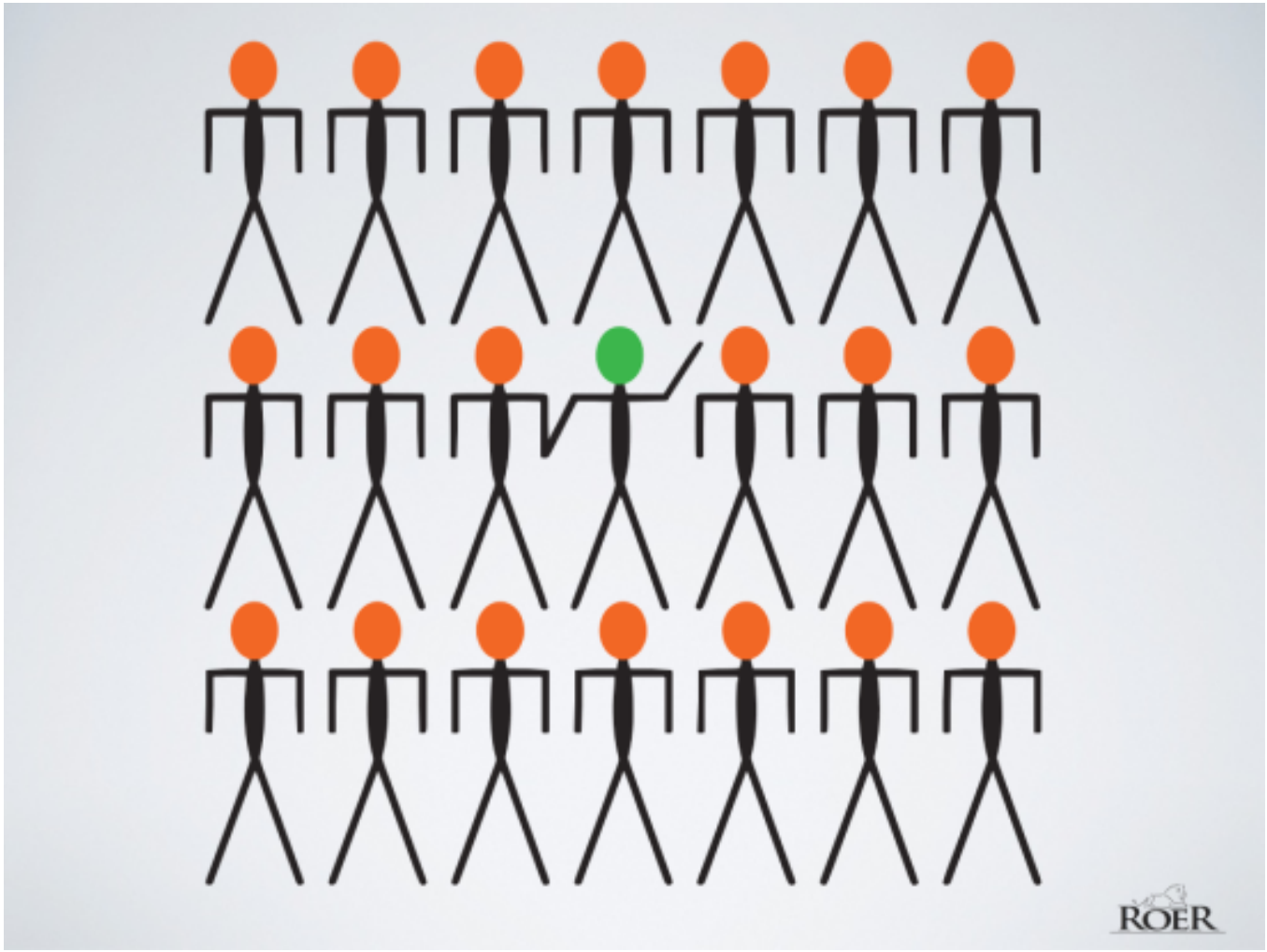


Red, Green and Orange – who are more secure?

Many security officers I know, tend to act like Red by alienating their colleagues, by expecting employees to understand security, without ever trying to understand the employees real job. Over the years, the Red ´s get disappointed by poor results, lack of support and becomes more and more negative and destructive – for himself, and for the organization.

Is this how you feel, perhaps?

Slide 13

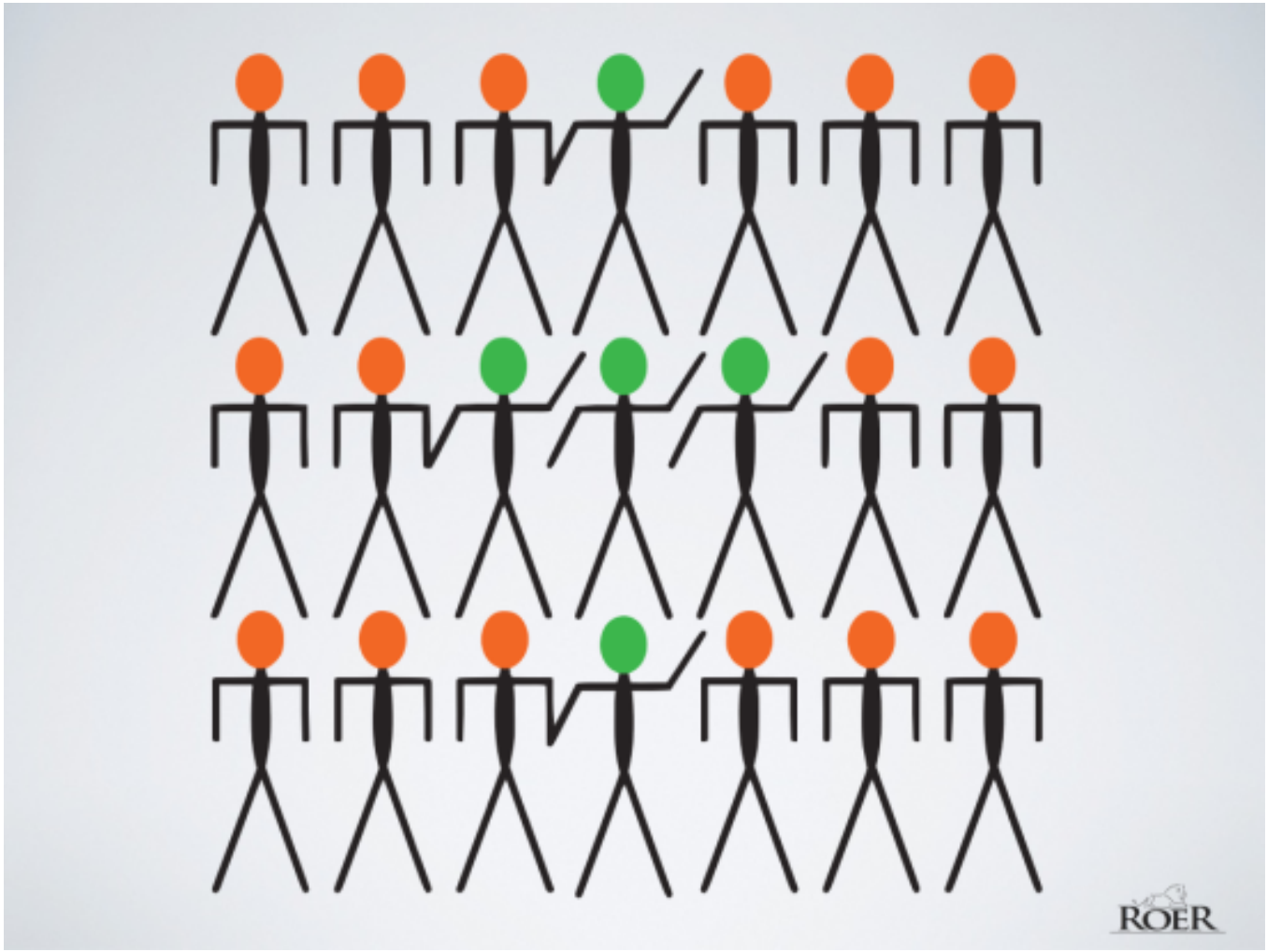


Introducing Green to the Orange group.

So let us take a different approach. Let us introduce Green to a group, and see what happens! At first glance, this look so much happier, I can feel the warmth all the way here! How will this go?

Remember that Green is introduced to a group without a strong, supporting culture, so he is able to more easily change its ideas, customs and behaviors.

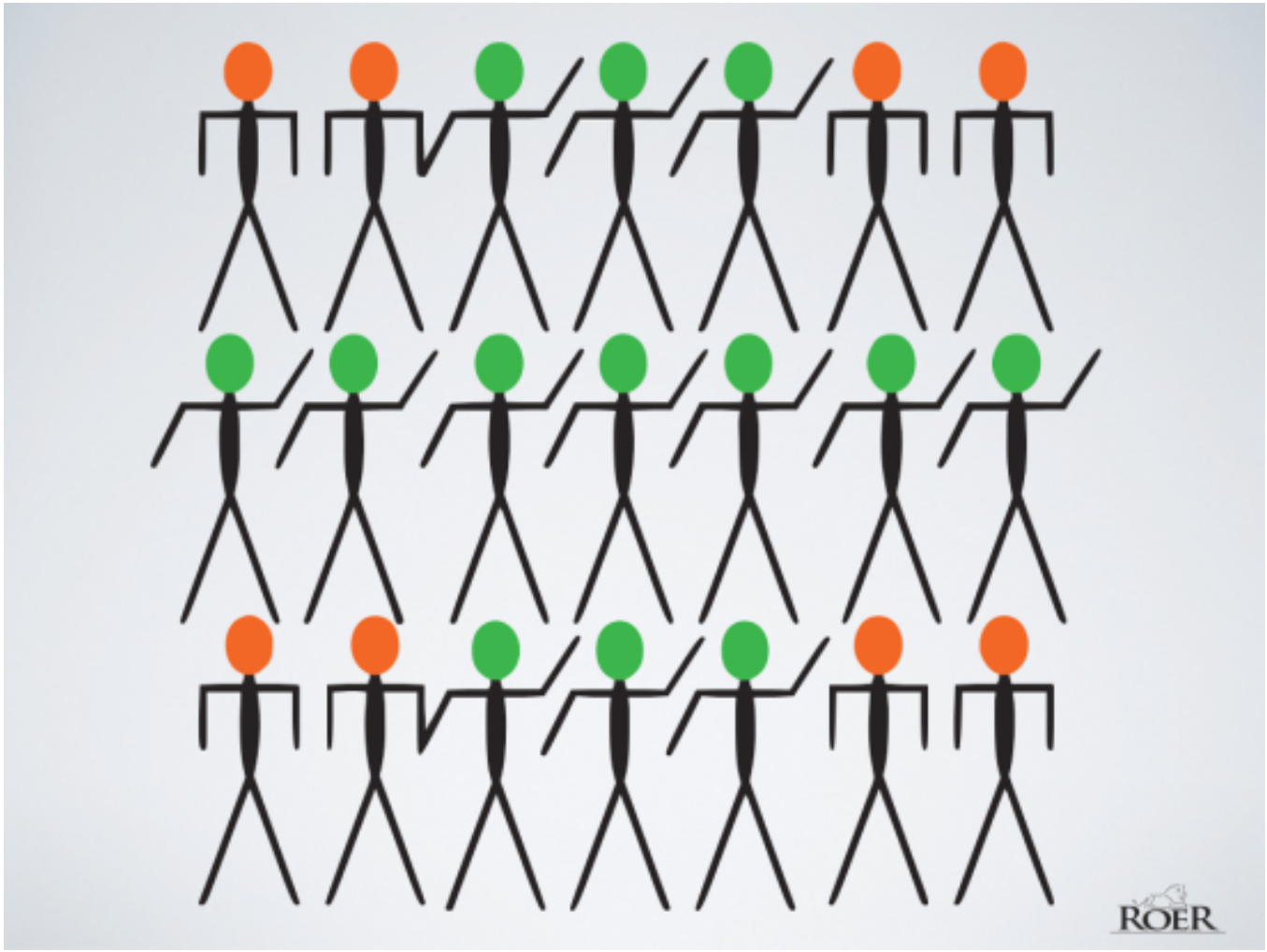
Slide 14



Green Joy!

Just like negativity, being positive is contagious. Being optimistic and looking for solutions instead of problems helps yourself, your team and your organization realize there may be a way out of whatever challenge you are facing. And as this notion spreads…

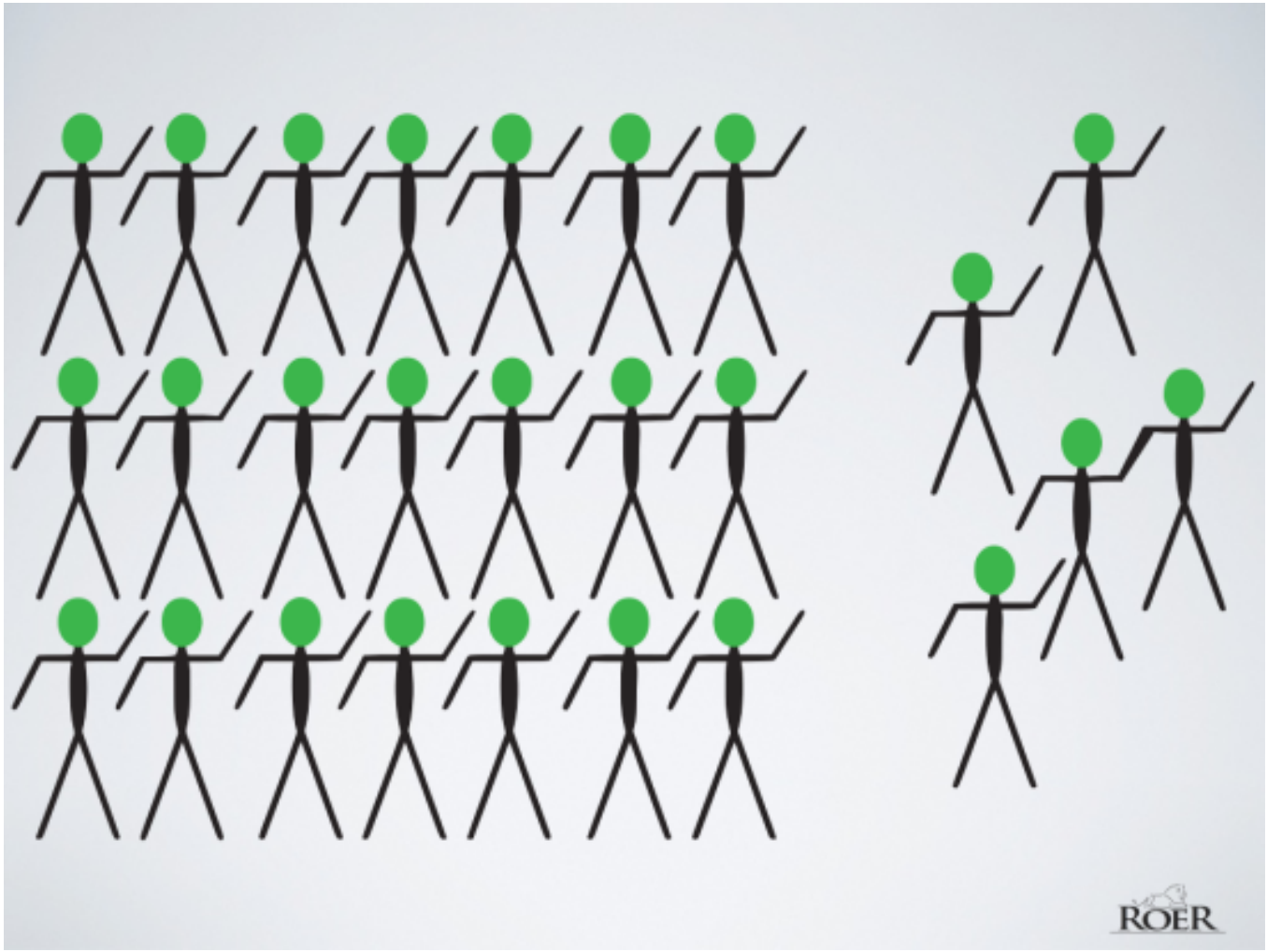
Slide 15



Growing positivity and care!

...more and more people will join the new culture.

Slide 16

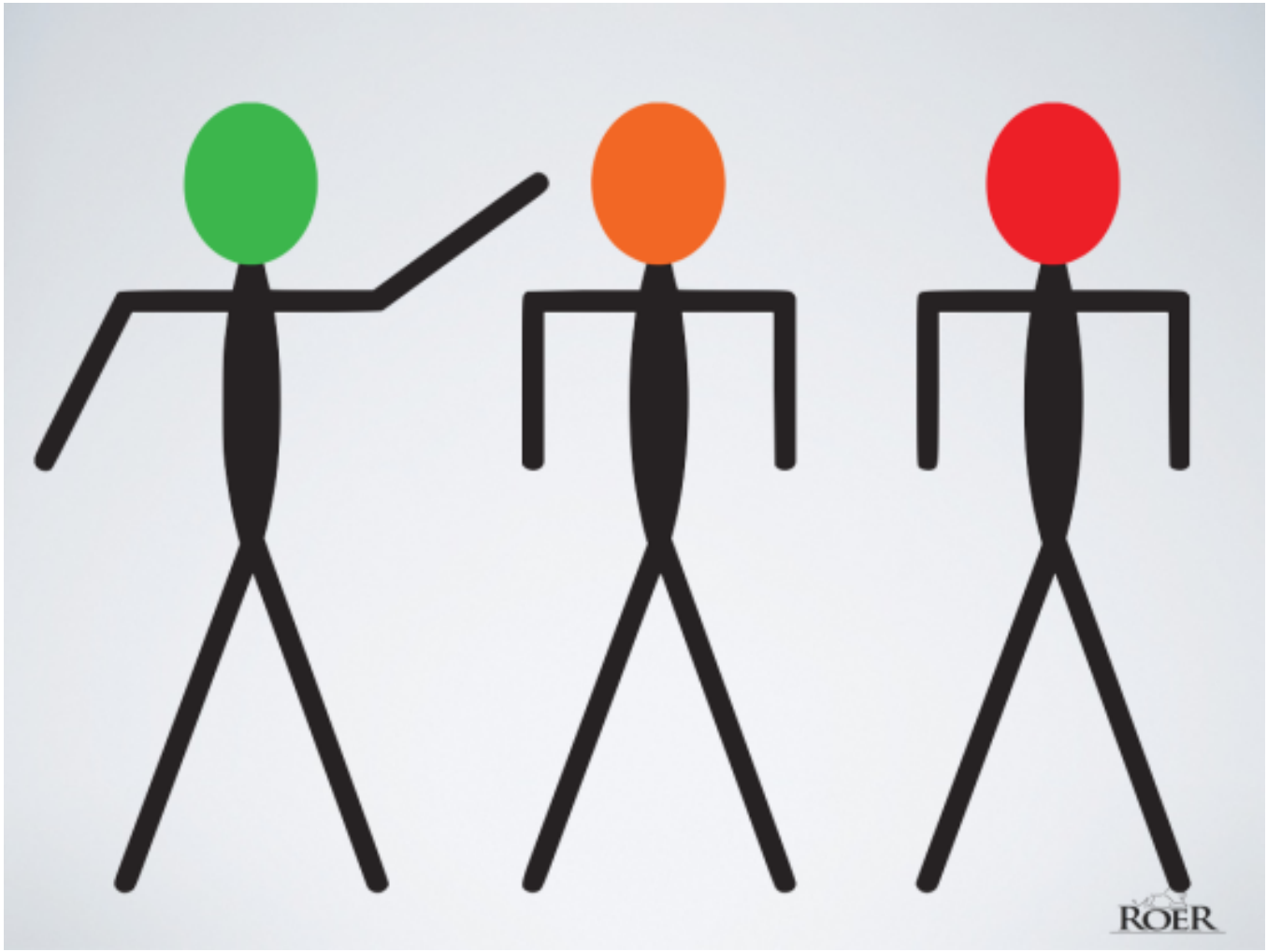


A positive culture attracts more positive people.

And as the culture grows, word is spread outside the organization too, attracting other individuals and groups with similar mindsets, with similar ideas, customs and social behavior. And you have created a magnet of positive attraction!

Why this matters to you as a security officer? Well, the insider threat have been reduced to the accidental incident of forgetting the Smartphone on Flytoget, a behavior that training and education can reduce – because this culture *wants* to learn, to grow, to succeed. This culture *care* about the group, and security becomes an integrated part of that culture. This groups *social behavior* allows it to build a better security through *understanding why*, by being *motivated for success*, and by *caring for each other and the group*!

Slide 17



Red, Orange or Green – which one do you want to be?

So the question is: Which security officer do you want to be?

- The negative, destructive force that is Red?
- The indifferent, easily changeable Orange?
- Or the positive, secure Green?

Let´s choose the Green, and let us build great security culture!

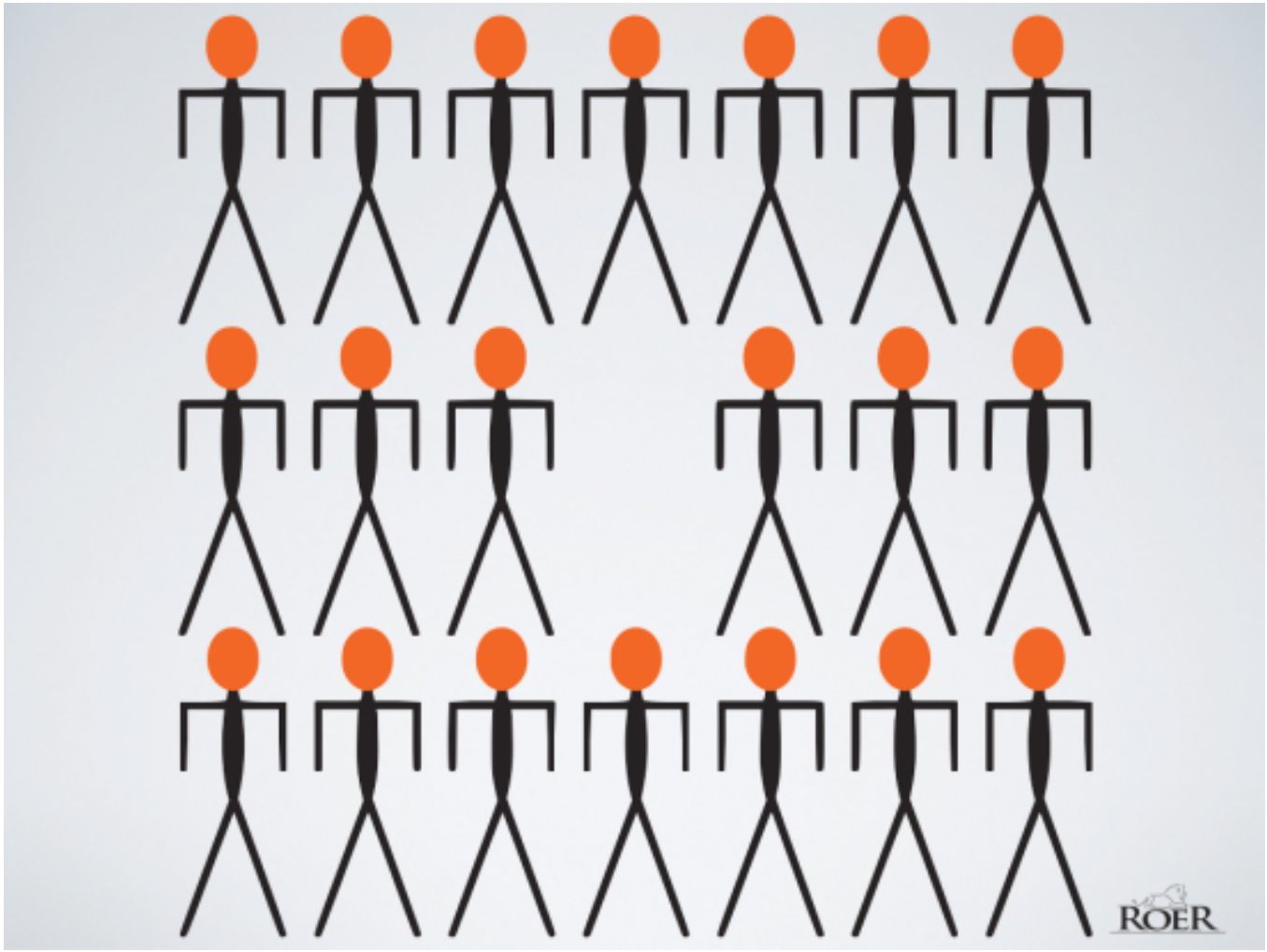
Slide 18

The definition of security culture.

Which brings us to the question – how do we define security culture? Using the Oxford definitions of Culture, and of Security, I have come up with this definition of security culture: *The ideas, customs, and social behavior of a particular people or society, that helps them being free from danger or threat.*

This in turn makes the job of the security team into the job of creating an environment that *helps the group* to being *free from danger or threat*. And we can do that by *working with* the ideas, customs and social behaviors of our team, department and organization.

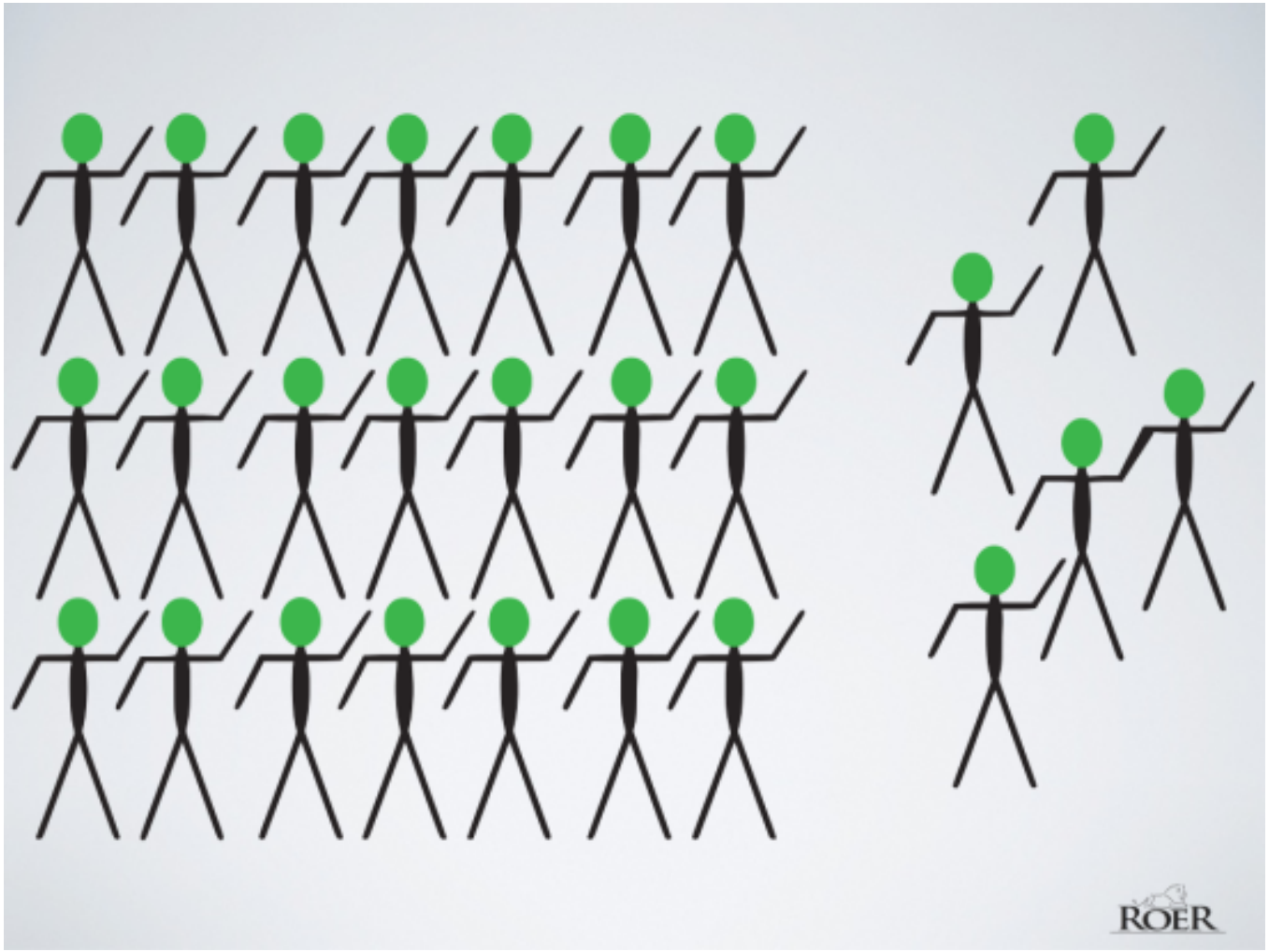
Slide 19



Go from Orange...

So we can make our goal, our purpose, to transform this...

Slide 20



...to green, positive culture!

...into this!

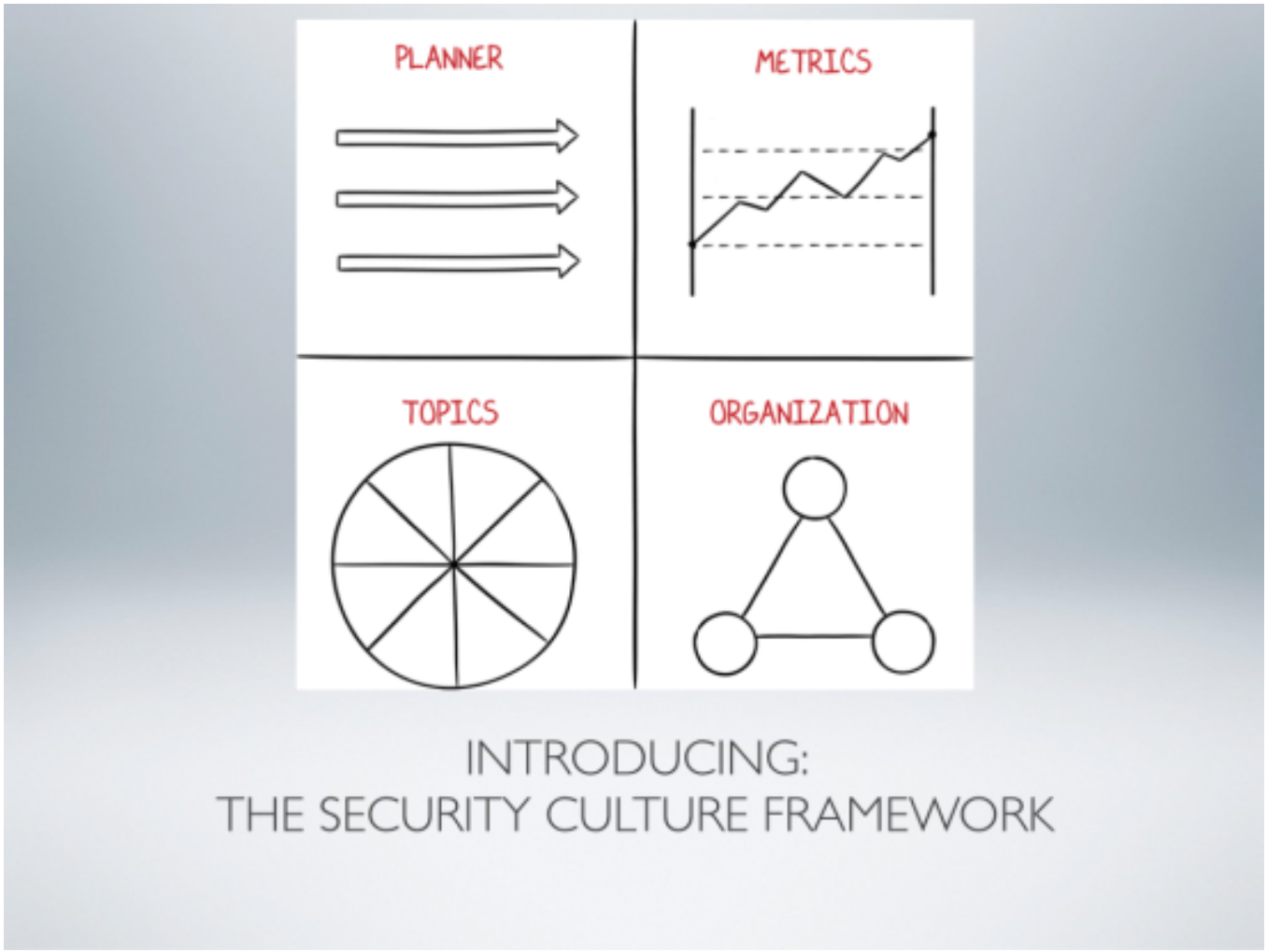
The good news is that we have already seen how culture can be transformed, and that should lead to the realization that *we* can curate that transformation. So let us do just that!

Slide 21

How to create a security culture program

Let us see how we can create a security culture program. It may sound like a daunting task, I know. Done correctly, using readily available tools and resources, it can be done!

Slide 22



The Security Culture Framework, a holistic approach to building culture!

One such tool is the Security Culture Framework. The Security Culture Framework consists of four building blocks:

- **Metrics**, where you define a baseline, set your goals, and define your metrics;
- **Organization**, where you organize your security culture workgroup, define target audiences and build organizational wide support;
- **Topics**, which are the activities your choose to implement in order to reach your defined goals; and the
- **Planner** where you plan your efforts, your revisions and your metrics.

Four areas that needs to be covered, each fulfilling individual tasks, while being connected to each of the others. You cannot have one without the others, and expect results – which is why most awareness trainings fails – they would sort under the Topics part, while being an important element, it is unable to create lasting change without the support of the other three building blocks required to transform culture.

With a framework like the Security Culture Framework, we can get to work:

Slide 23

A step-by-step guide

If you want to walk a thousand miles, you start with one step.

When building security culture, we have found that these steps are a great first step.

Setting up your team is where you build a security culture work group. You want to include the kind of expertise you are unlikely to have yourself – especially from HR (training and organizational knowledge), and from Marketing (creating the story+presenting it).

Together with your team, you define your goals, and decide how you know that you have reach them (or missed). You need to measure your current status too, so you know where you are. You will use the Current situation and compare it with the desired goal to make a GAP-analysis to help you determine which elements, topics and activities you will use in your security culture program.

Then you define your target audience. Again, here the marketing guys can help. Why, you may ask? Consider the differences between the IT-department and the sales people. They are quite different, right?

Then you start choosing the topic(s) you want to focus on (remember your goal), and activities that will support your message. Again, Marketing Dept.!

Plan your efforts – think of each effort as a campaign, make it last a limited time, which will allow you to measure before- and after-effects. Which is the next you do – measure, learn, change and do it all again!

Slide 24

A program is required.

Now that you know why culture matters in security, and how to organize your work, let me explain why you need to create a security culture program.

Culture is changing and evolving all the time. As we saw earlier, individuals impact culture, and culture impacts individuals. We need to run an on-going program to nurture and control the change we want.

Also, when so many security officers complain that their awareness trainings fail to yield results, one of the reasons is that they fail to see the need for a holistic approach, a program where a training is *one part* of the whole, not the Silver Bullet to solve it all!

Slide 25

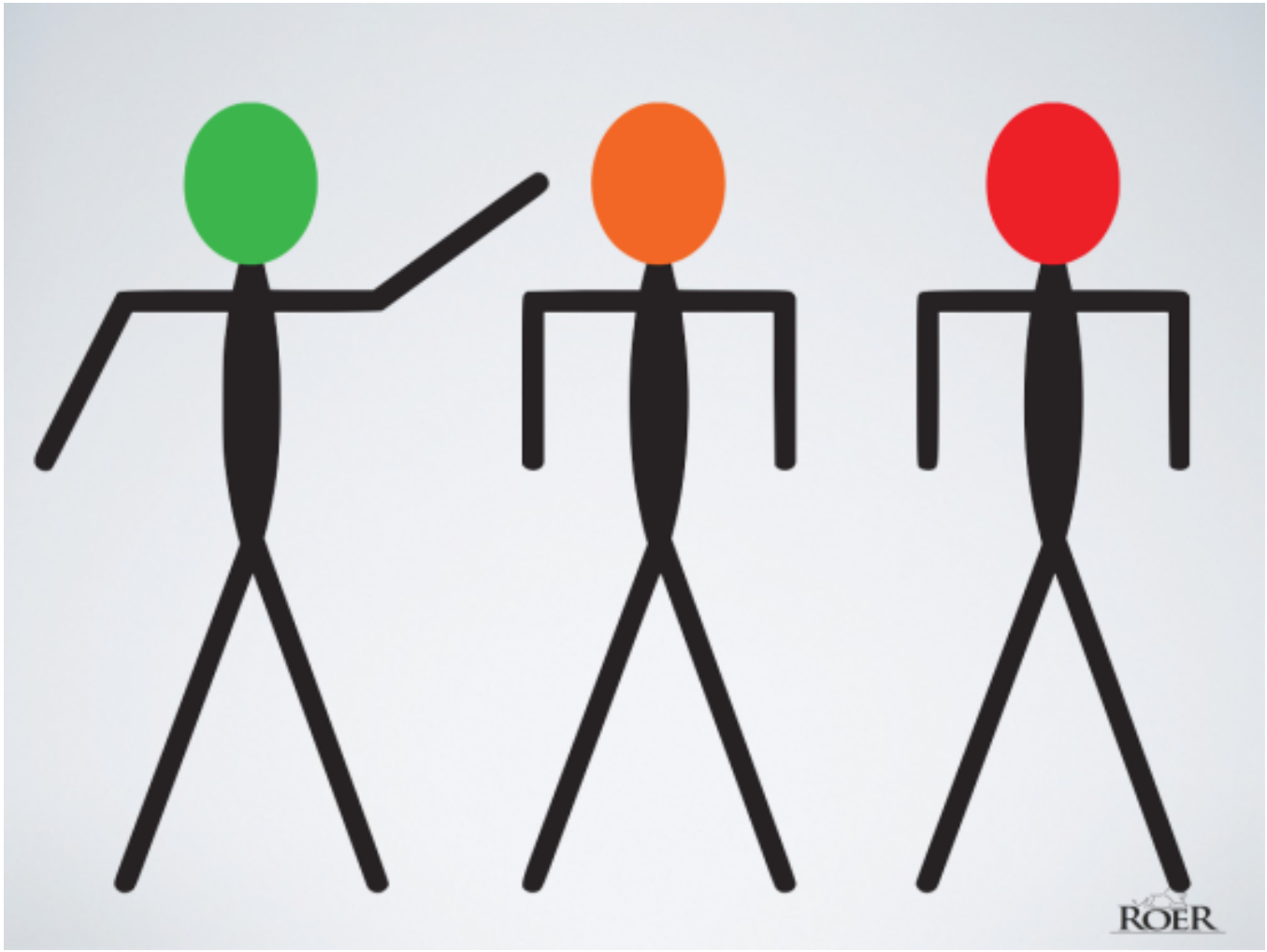
And there are no silver bullets!

So to create successful security culture, a positive one, driven by the Green, you need to nurture the culture. Make it support business, your job is to secure the business, right? Create both understanding *and* awareness, and a support structure where your colleagues knows what to do, and whom to turn to, when they make a mistake.

A security culture program is an on-going effort, one that never stops. We can say that security is built-in to culture, that culture is a security measure to create a stable, safe environment where we are free from threat. At least we shall consider that our goal!

And remember that every walk starts with one small step! You can do it too!

Slide 26



Red, Orange, Green: Your choice, your responsibility.

So the question remains: Which security officer do you want to be?

I know who I want to be!

Slide 27

Thank you ISACA Nordic Conference 2014 for inviting me.

Thank you very much! I will be available for questions this afternoon. You can also reach me on Twitter, and my blog.

Of course, you can buy some of my books too – they are on amazon.com!

Thank you!

Slide 28