JUTA
POPIA PORTAL

ISSUE 2 • HACKING DATA BREACHES: WE NEED A NEW BREED OF COMPLIANCE OFFICER • SEPTEMBER 2019

1. OVERVIEW

We list the knowledge and skill requirements necessary for Compliance Officers to properly manage their organisation's Information Security and what organisations need for adequate Incident Response Management.

2. **HACKING DATA BREACHES:** WE NEED A NEW BREED OF COMPLIANCE OFFICER

R58.4 million. According to IBM, that was the average cost of a data breach in 2020. It is no surprise then that **cyber resilience is top of mind** for CEOs worldwide. But what does this mean for compliance officers? What should we be doing to address data breaches? And what are the skills we need to get it done?

To effectively protect your organisation from data breaches (or pick up the pieces if it has already happened), compliance officers need to reinvent themselves – these are the lessons we have learnt.

2.1. GET THE RIGHT PERSPECTIVE

Get your head out of your …
for compliance to thrive, you need some perspective on what we refer to as the compliance PR problem. Compliance was best summed up by **Sean Graham:**

> ***'Compliance is like a colonoscopy: People may need it, but they don't want it, they don't like it, and they certainly don't want to talk about it. (And they absolutely don't want any more than is necessary).'***

2.2. GET THAT THIS IS NOT AN IT PROBLEM

All too often, information security is dismissed as IT's problem. This causes two problems. First, treating cybersecurity as a tech problem usually leads to the thinking that we need to be looking for a tech solution.

'The security problems we're now facing can't be fixed with products alone. We can't fix them with more security analysts any more than a retailer could fix shoplifting by assigning a security guard to watch every shopper as they wander around the store.' – Adrian Sanabria (one of the good hackers)

Second, by relegating information security to IT you train your staff to think that it is not their responsibility, because 'someone else is taking care of it, right?' The truth is that a significant number of breaches are caused by humans and not IT, error, and no piece of tech can prevent that.

2.3. AIM FOR CONSCIOUS INCOMPETENCE

The internal auditor at one of our clients made a joke the other day (yes, it happens). She said that managing risk is all about moving from unconscious incompetence to conscious incompetence.

This is also true of information security.

> ***'One of the main cyber risks is to think they don't exist. The other is to try and treat all potential risks. Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats. Think data, but also business services integrity, awareness, customer experience, compliance, and reputation.'***

– Stephane Nappo, Global Chief Information Security Officer, 2018 Global CISO of the year.

To do information security management properly, we believe compliance officers should have a working knowledge of the following areas:

- Risk management: Managing uncertainty and making educated decisions.
- Information security management and data governance: Protecting the confidentiality, integrity, and availability of information.
- Business continuity management: Keeping your organisation's doors open when the pawpaw hits the fan.

Does this mean that compliance officers need to be proficient on all these topics? No. It is about conscious incompetence, remember? You need to be able to ask the right questions and collaborate with people who are experts in these areas.

2.4. NO POLICY IS BETTER THAN A BAD POLICY

Too many organisations still write policies that are never implemented. What we mean by that is that the policies are there, in a folder somewhere, but no one follows them, compliance isn't measured in a meaningful way, and there are no consequences for non-compliance.

What does it mean to implement a policy? Well, you can start by asking these questions:

- How does the new policy impact our existing policies and procedures? Do we need new ways of working?
- What is the impact on infrastructure and equipment? In other words, do we need new buildings, equipment, hardware or software?
- What is the impact on people? Do we need new people, do the existing people need new KPIs (have we added to their job)? Do people have the skills to do what we are asking of them? Do they need training?

2.5. LEARN MORE ABOUT PEOPLE

When it comes to information security, we like listening to what hackers have to say:

> ***'The methods that will most effectively minimize the ability of intruders to compromise security are comprehensive user training and education. Enacting policies and procedures simply won't suffice.'***

– Kevin Mitnick, convicted hacker

Luckily, there is a wealth of research out there about what makes people tick and how to change behaviour. It is called behavioural economics and here are two of our favourite books about it:

- Thaler, R.H & Sunstein, C.R. (2009) Nudge: Improving Decisions about

juta

Health, Wealth, and Happiness. London: Penguin Books.
- Kahneman, D. (2011). Thinking, fast and slow. New York, NY, US: Farrar, Straus and Giroux.

> ***'Although we generally perceive fear as an emotion, it is actually a social construct: for someone to be scared of a tiger, in the first instance they have to understand what a tiger is and to comprehend the danger it poses to them.'***
>
> – Dr Jessica Barker, a specialist in the human side of cybersecurity.

2.6. HOPE FOR THE BEST BUT PLAN FOR THE WORST

Feel like saving R17.7 million? **IBM's study** in 2020 about the cost of data breaches reveals that companies who pay attention to incident response management and test their processes saved R17.7 million per breach. If that won't turn your board's head, we don't know what will.

Here is what you need:

- an incident response policy and procedure;
- an incident response team (including external infosec specialists, forensic auditors, etc.);
- disaster recovery plans (cyber resilience and fault-tolerant systems and processes);
- disaster communication specialists on hand (this is a specialist field – many marketers suck at it);
- an attorney to help you with your notification to the Regulator and to preserve evidence (privilege must attach);
- procedure and IRT testing and testing both again; and
- training (nudge) for your employees and then train them again.