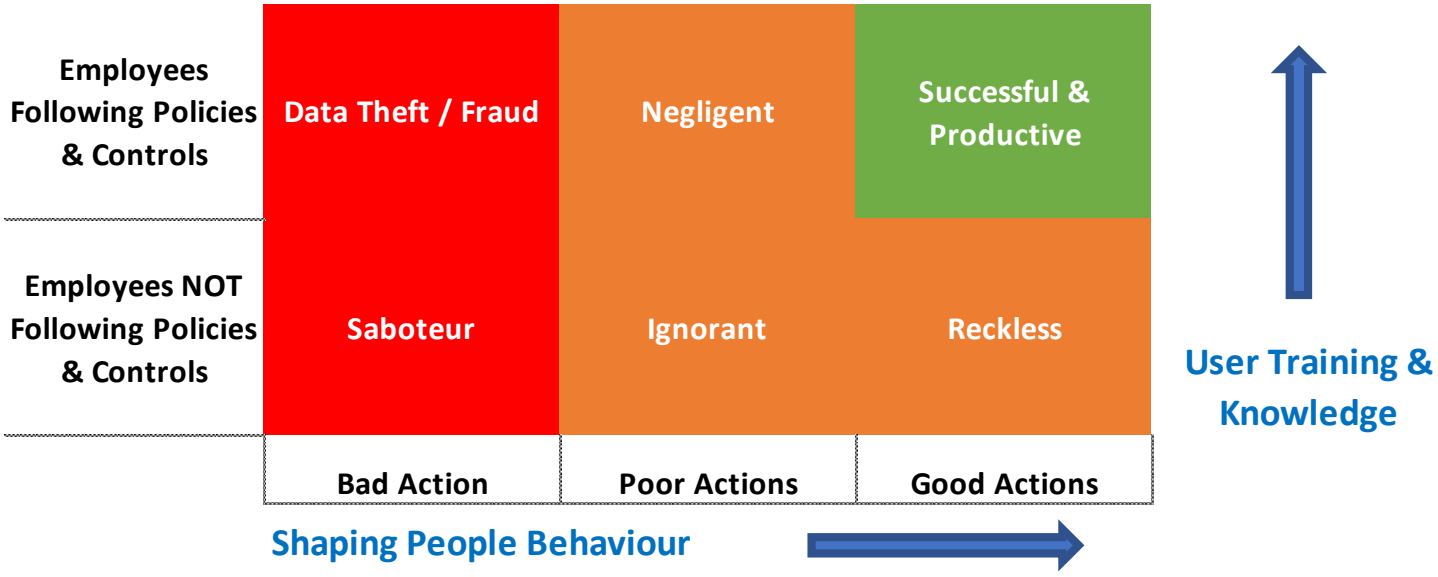
Does Staff Behaviour Signal Your Organisation Risk Exposure?

"We are what we repeatedly do. Excellence then, is not an act, but a habit"
- Aristotle

Many businesses aim to hire trustworthy, loyal, hardworking, and conscientious employees who will carry out their duties to the best of their abilities. Developing trust with your employees is necessary since it has a direct impact on office security. It can be hard to see how employee behaviour can place a business at risk but all businesses face a certain amount of liability with the employees they hire.

To better understand the risks, it is a good idea to classify your employees based on the qualities and behaviours they exhibit. In fact, you can effectively mark the six general behaviours that many employees display into the following boxes on the chart given below



The Green Box

The green box signifies a successful person or a model employee. These are people who are dedicated to the organization. They share the same values, the same aspirations, goals and objectives as that of the business. They are also more likely to follow policies and have a healthy understanding of good security practices. Organizations actively seek out such people because these people contribute to creating a work environment that is productive, secure and engaging.

The Orange Boxes

The orange boxes are a mix of the reckless, negligent and ignorant employees that a business might have:

- **Reckless** - These are people who act without thinking. Despite the fact that they are aware of the dangers, their reckless behaviour can increase organizational risks. These people are most likely to spend considerable investment on additional resources and yet are not helping organisations in becoming resilient. **For example**: They will gladly attend a cyber security awareness course, and yet fail to follow policies & controls.
- **Ignorant** – These are employees who don't know any better. Their knowledge of corporate security practices is limited and outdated. Poor knowledge also translates into silly actions that can be disastrous for a business's security infrastructure. **For example:** They are likely to pick up a random USB and plug it into their computer or they might share sensitive information on a public website or more likely click on a malicious phishing email or open a malware attachment. Lack of proper training from the workplace can also lead to this aspect.
- **Negligent** – These are employees who fail to act properly despite knowing better. Employees can be negligent when they are overworked. They might also be preoccupied, overly stressed

and disengaged because they just don't like working there. **For example**: They might send out sensitive information to a cloud storage provider against corporate policies, simply to be able to complete work from home or they may send sensitive personal information via email.

Many employees usually fall into the orange boxes in an organization but very few are ever reckless.

The Red Boxes

On the other hand, there are some employees who are firmly in the red boxes.

- **Saboteur** – This refers to an insider who brings direct harm to an organisation assets or an individual. These crimes are committed by technically sophisticated people that know the machinations of the organisation extremely well. Such sabotage activities are performed as a result of being highly disgruntled, dissatisfied and have unmet expectations from their organisation. Most of the insiders that have committed such attacks have a personal disposition.
- **Data Theft** – This refers to a person who chooses to steal proprietary information from the organisation. This also includes espionage. Interestingly, very few steal data to sell the information. They steal the data because they either want to take it with them to a new job or start a new business. **For example:** A salesperson who walks out with the organisation's list of contacts, or a person leaving to a competitor with proprietary information and processes.
- **Fraud** – This refers to a person who makes use of unauthorised access to modify, delete or manipulate organizational data for personal gain or theft. This can cause loss in revenue, identity crimes and more. **For example:** A person who illegally receives money for authorising new driver licenses and pockets the amount. In another example, a payroll officer can steal business funds by adding false transactions.

Now that you know the kinds of behaviours and risks that you can potentially face, you need to work out a solution. To do this, you need to identify how engaged your employees are. A good gauge is to understand whether the corporate policies that you have in place are being followed. If you notice that your employees are actively avoiding your policies, you have to find the main reason behind such behaviour.

Why Don't Employees Follow Policies?

Many businesses believe that their employees don't follow the policies because they just don't care, but that is not the case. The following are a few major reasons employees might not be following your policies:

- **Poor Training** – Not taking the time to train a new employee in accordance with the standards enforced by your business can make a marked difference in the kind of work they do and the risk you face. With poor training, an employee will have to fall back more on the training they received with other businesses, which might not be suitable for the current workplace.
- **Lack of Motivation** - Poorly motivated or negatively motivated employees don't follow policies because they don't feel the need to improve. They won't be self-motivated to work nor will they

be likely to correct their behaviour if they are warned about it. Poor engagement can increase your turnover rate and make it difficult to retain employees properly.

- **Unmet Expectations** Employees have certain expectations from their workplaces and if these are not being met, you can face bigger risks. Businesses that use a stick and carrot approach, but fail to deliver on the promise are the ones where this is more likely to occur. When employee expectations are not being met, you can't keep pushing them to continue meeting the ever rising expectations that your business has placed on them.
- **Disengagement** – In some cases, the employees might be getting disengaged with their work because they don't like their job. If left unchecked, their dissatisfaction can turn into dislike for the business. In turn, it can lead to employees being more brash, abrasive and dismissive of the policies, rules and regulations the expectations of the business. According to the State of the Global Workplace, reports that 85% of employees are disengaged, of which 18% of employees were actively disengaged.
- **Poor Communication** – Communication is a key component in establishing a healthy work environment and sometimes, policies might be getting ignored because a person is not aware of them. If no one bothered to explain these properly to them, the employees will rely a lot more on their understanding of the policy instead of what it truly means. In such situations, confusions, misunderstandings and more can easily arise, causing more issues and security risks.
- **Too Complicated** – A lot of times, businesses have policies that are convoluted, complicated and unnecessarily long. In such cases, employees might either opt to shorten them by cutting out a few steps, or they might avoid following them completely. In general, the easier the route is to something, the more likely it is that it will be used. A confusing policy, especially when the employee is pressed for time or stressed out, can be too much hassle to deal with. Policies are there to help the business and employees perform a service; if it is just complicating things, it could be a sign of poor policy.

All these factors contribute to making employees be more careless or dismissive of the policies that are being enforced.

Taking Positive Measures

Organisations need to care about the employees because they are a key component of the business. Most businesses, don't always realise this factor until it is too late. Luckily, with careful training, workshops, group discussions and team building activities with employees, you can easily help them understand the risks as well as develop a productive work environment.

Workshops and Trainings

Actively engaging with your employees through workshops and training can be vital in helping to shape their behaviour as well. To change unwanted behaviour in employees, businesses need to be smarter about their approach. You can either choose to sign up for workshops or have workshops organized with a professional company that allows you to train your employees onsite. Regular training plays a bigger role in ensuring that your employees are meeting industry standards and also know how to provide

services in accordance with the policies of the business. A good idea is to work with a professional company that specialises in this aspect. While it might appear rather costly to you, think of it as a long-term investment. By investing and improving the behaviour of your employees, you get to enjoy better benefits, including increased productivity, better engagement as well as fewer security risks.

Get Our Help

If you are looking for a company that specialises in helping you to minimise the "human element" risks for your organisation through specialised security assessments, workshops, employee trainings and more, get in touch with CommsNet Group.

You can also sign up to CommsNet Group news update to get more information and resources on regular basis.

Your Next Best Step

If you are now keen in addressing the risk from within, why not attend our free public Insider Threat Worksop. These half day workshop are conducted in most capital cities and are designed to help you understand the best practices that can be implemented to identify and mitigate insider threat within your organisation.

We also provide a customised Insider Threat Workshop specifically designed for organisations. It differs from the public workshop by because it is tailored to you. The actual workshop consists of two days where we help your team develop a strategic action plan to address the risks of inside threat in your organisation.

To find out more about our Insider Threat Workshop

Contact Us

if you need some more resource material, download the Insider Threat eBook by CommsNet Group, completely free of charge. For more information, you can also send them an email at: info@commsnet.com.au OR give us a call at: +61 26282-5554.