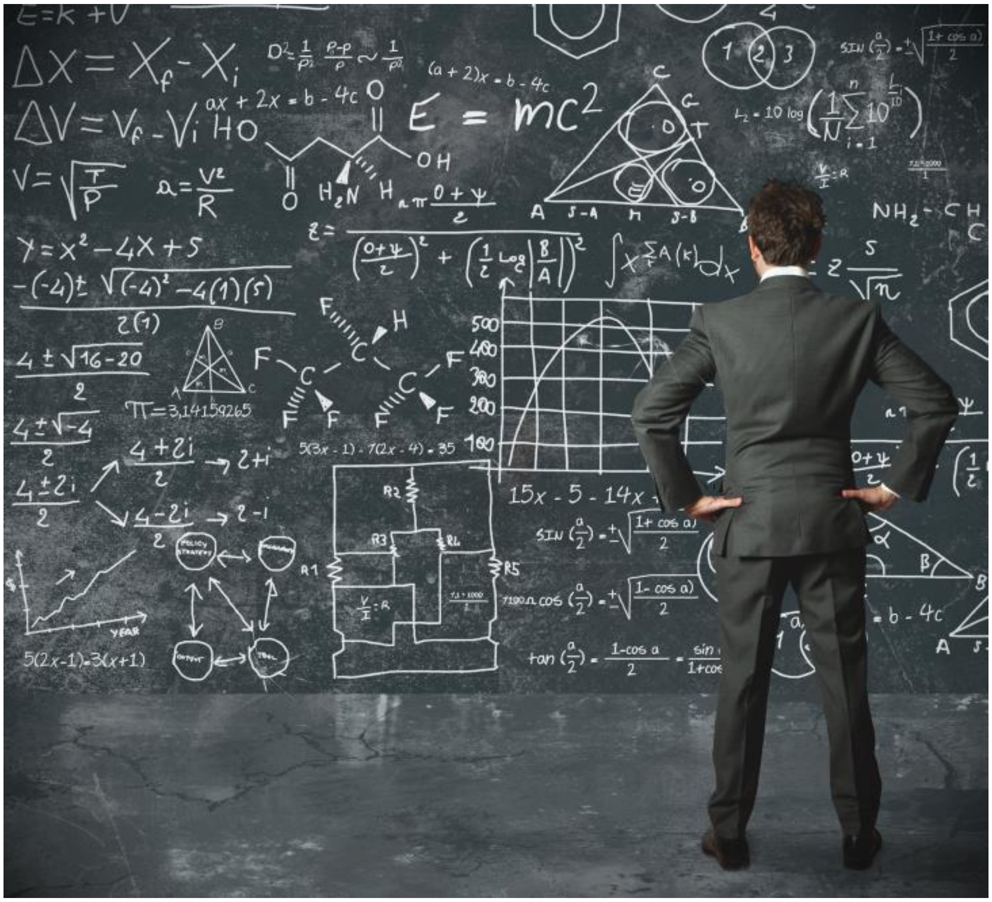
When It Comes To Security Simplicity Is Always Better Than Complexity



"If You can't Explain It Simply, You Don't Understand It Well Enough."

- Albert Einstein

We all know “**simple**” when we see it, touch it, or use it. It gets to the core of what things indeed are with little effort.

On the other hand, complexities we encounter everyday force us to limit our visual consumption, to dismiss, discard and ignore things we don’t instantly connect with.

Johny Ive (ex-Chief Design Office for Apple) once said - “*simplicity isn’t just a visual style. It’s not just minimalism or the absence of clutter. It involves digging through the depth of complexity. To be truly simple, you have to go deep… You have to deeply understand the essence of a product to be able to get rid of the parts that are not essentia*l”.

There is power in simplicity. We know it. We see it. We feel it.

If you are into sport, you will be amazed by Lionel Messi or Michael Jordan skills. Both can take the complexity of their sport and make it look “artless”.

If you are into music, composers such as Wolfgang Amadeus Mozart made music into such simplistic and memorable harmonies that they are with us forever. Such as “twinkle twinkle little star” which is based on his twelve-bar variation composed in 1780.

In essence… the easier something is to understand, the easier it is to share it. And the easier your message is to share the more people you can impact.

But simplicity does not mean easier.

And it’s important to realise that in the words of Steve Jobs:

“Simple can be harder than complex: You have to work hard to get your thinking clean to make it simple. But it's worth it in the end because once you get there, you can move mountains.”

The world around us is changing at a rapid pace. Complexity is increasing significantly in this increasing interconnected, digitization and data sharing world.

Today, simple tasks like using a credit card, a phone, or a computer now provide an opportunity for miscreants to take our money, our identities, and cause significant severe disruption to our lives.

Unfortunately, our neighbour is now the entire globe.

As the world evolved and became more technological, attacks evolved along with the new developments.

Let me ask you today… what do you think when you hear the word "**security**"? Do you think of security arm guards, dogs, fences, monitoring cameras or do you think of firewalls, a myriad of security software tools, malware, hackers, data leaks, regulation, cryptocurrencies, cybercrime and more?

It is not a surprise that we have developed an equally evolved, complex cybersecurity system.

One Australian organisation told me that they were managing at least 28 different security technologies for an organisation the size of 1,200 staff.

It's no surprise that this organisation was struggling to deliver real effective business protection and value.

The world of complexity is particularly problematic. It hinders innovation, collaboration and the ability to share information. It suppresses development and hampers customer services. It creates confusion and misunderstanding.

When a business becomes more complex, it can become siloed. This results in employees focusing on their core work to the detriment of others. It builds mistrust and competition within rather than the benefit for the entire organisation.

So, why is security so hard and getting harder?

Look around, and there isn't a single organisation out there that hasn't increased their investment in protection solutions to prevent from being breached.

However, these efforts are falling short of what is required. Whether you are a small, local business, a global conglomerate with extended supply chains, an individual with a mobile phone, or a government department responsible for national security, your level of exposure and responsibility to prepare for threats are both increasing rapidly.

More technologies do not mean better security!

The 80/20 Way

I’m sure you have come across the 80/20 rule... Which states that 80% of your results come from 20% of your efforts and 20% of your results come from the other 80%.

Another way to look at it is:

- 80% of your security protection comes from 20% of your security investments
- 80% of your security incidents come from 20% of people.
- 80% of your external threats come from 20% of the same source.
- 80% of customer service headaches come from 20% of the “problem children”.
- 80% of warranty claims come from 20% of the product defects.
- 80% of your productivity comes from 20% of your tasks.
- 80% of your traffic in your city is from 20% of your roads.

I could continue, but bear in mind it’s not the exact number 80/20. **It’s the principle**. Sometimes it's 60/40 or 70/30. Sometimes it is 95/5.

If 20% of your investment provides you with 80% of the protection, why not align your security strategy to this paradigm?

Let's take it to another level. If you only look at the 20% of your security investments and then apply the 80/20 on that. That means 64% of your protection is derived from only 4% investment.

There is magic here if you take the time to realise this power.

Given that we have shrinking budgets and resources and yet we are asked to do more, comply more, or treat more attacks, we need to realise that continuing investment in security tools will not necessarily add protection to your business. All you are doing is adding complexity.

Everything that matters in the business or anything that you can measure **isn't linear**. It's exponential!

How Can We Help you?

It is interesting to note, that majority of security budgets (more than 80%) of organisations these days goes into security tools to prevent only 20% of the security threats.

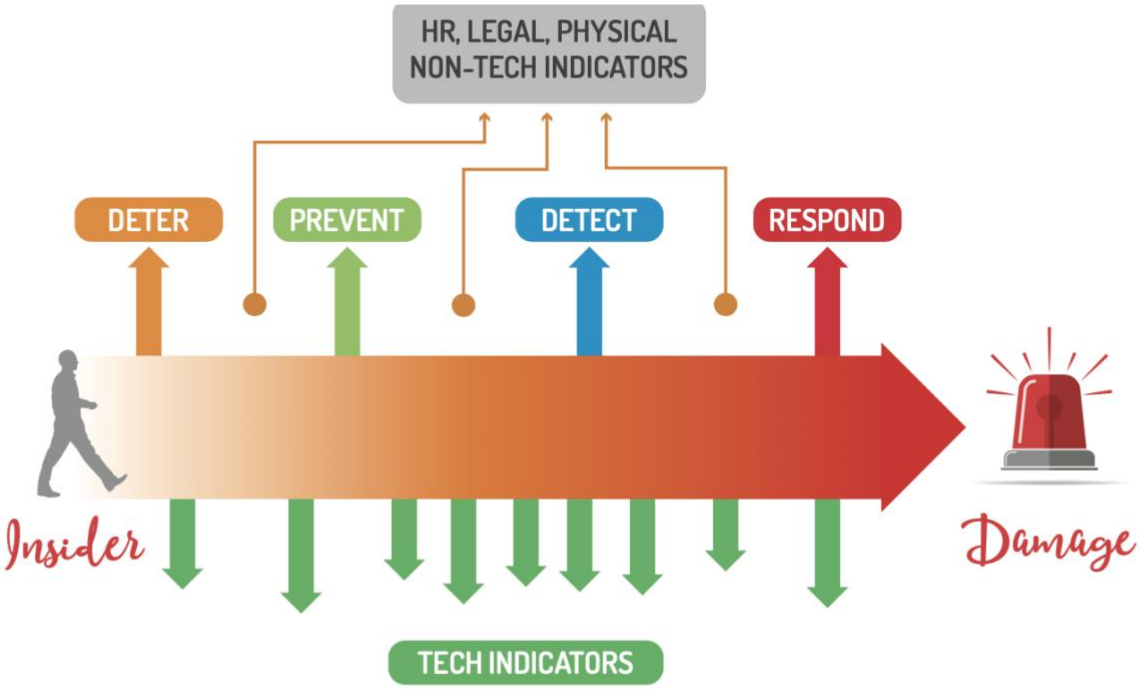
In 2015, Verizon Data Breach Incident Response stated that "*90% of all incidents are people. Whether it's goofing up, getting infected, behaving badly, or losing stuff…*"

If not to state the obvious, **security is all about people**. Even cybercrime is about a crime committed between people who use technology.

To get the simplicity in your security and governance, you need to consider the human element of security. That's what we specialise.

We can help you:

1. **Shaping behaviour of people, positively** so that they act in the best interest of the organisation and reduce your organisation exposure either intentionally or accidentally.
2. **Focus in maximising your return on your security investments by simplifying your strategy.**



Contact us by filling out the form of the CommsNet Group website to discuss your requirements: https://commsnet.com.au/contact-us