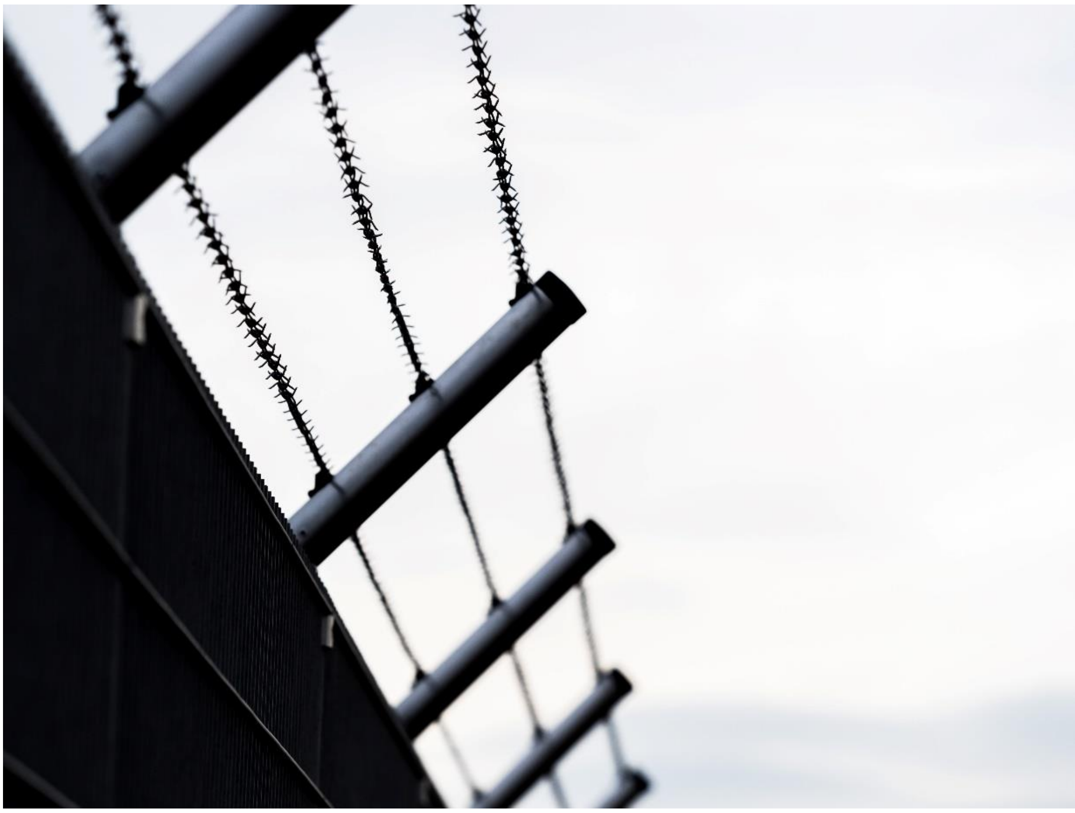
# Don’t forget the fundamentals of security

Ian Edwards MBCS, Head of Information Security & Risk at MEDICA Group reminds us about not losing sight of the fundamentals of security, amongst the backdrop of a technology-driven world.

I was born in the mid-1980s a few years before the first worm and anti-virus tool was created. They were harmless and borne out of a research project by Bob Thomas and developed further by Ray Tomlinson, the inventor of email. I always find it exciting to look back and see how far technology and associated threats have come. I’ve been privileged to grow up and see the digitisation of the world around me.
If we fast forward, security threats and actors have caused significant damage to industry, public services and commercial organisations. This has become more prominent and the peak of this is not yet visibly clear.

## Information security fundamentals: Part 1: Principles



When thinking about information and cyber security fundamentals we are often drawn to our underlying principles. The confidentiality, integrity and availability of information or the CIA triad as it is often referred to. These principles are well established and should form the backbone of any security programme or framework.

## Security technology and culture

I recently attended one of the larger security conferences in London and it touched a nerve for me. Although I’ve seen the vast maps of established vendors and start-ups, I’d not previously attended a conference with over 400 brands on show. Now, I am not aiming to vendor bash here. Each business provides one or more solutions and ultimately target specific risks. A large portion of these solutions tend to be pure technology and will be seen as shiny and attractive to IT and security professionals.
Over the years, I believe the industry has developed a ‘sheep like’ culture that can be likened to our everyday lives. I entered my teens in the late 1990s and there was a strong culture of association with

brands. If you weren’t wearing the latest Nike, Kappa or Adidas track suits, you were often looked down on. I’m very proud of my parents as they never succumbed to the pressure (and ludicrous prices).
Fortunately, I was a grounded young person and mature enough to develop my own identity. I was the kid who would wear generic jeans and a t-shirt instead of a tracksuit and was comfortable wearing a less common ‘brand’. My parents’ approach to life has been an inspiration to me. They focused on getting the basics in life right. This predominantly consisted of managing the family finances to ensure we could live, enjoy our time together and enable my sister and I to grow up positively.
This leads me onto the point I am trying to make here. Whether your business is young or established there is no specific ‘brand’ of security or technology that you should follow. However, and this is a big however; there are certain fundamentals that apply to all.

## Information security fundamentals: Part 2: What do we consider fundamentals to be?

Earlier, I reminded you of the traditional CIA principles. If we look at our security programmes or frameworks, what do we really consider as the fundamentals? If I think of the word fundamentals, I’m led towards ‘basic’ or ‘essentials’. No matter the context, the fundamentals is about getting the basics or essentials right. In our personal lives this usually means:

- Generating a steady income.
- Providing for oneself or a family.
- Protecting ourselves and our family.
- Supporting those closest to us.

If we consider this in the business context:

- Generating revenue.
- Providing a reliable service or product.
- Protecting business assets.
- Supporting staff and customers.

The two themes are very similar. If we look at the security context:

- Enable the business to generate revenue
- Enable the business to provide a reliable service or product.
- Enable the business to protect its most important assets.
- Enable the business to support staff and customers.

You can see this is all about enablement, advice and providing layers for the business context to be successful. Obviously this is highly simplified and there is of course much else to factor in. You’ll be expecting to see ‘Information security fundamentals: Part 3’ coming up. Instead, I’ve broken down some key examples that I consider as security fundamentals...

## The human factor (people)

There is a revival in the industry at the moment. I’ve met a number of passionate individuals whose goals are to advocate the importance of the human factor. I personally believe this is one of (if not the most) important areas of information security. As people we are always targeted by threat actors at home, work or when out and about. Phishing, as an example, still remains one of the largest attacks against us, yet general awareness and understanding of this still remains a huge issue globally.

Developing the human firewall is often one of the lowest cost security controls. It is more than just providing annual refresher training, though. Knowledge and understanding can only be acquired over time. If you are forcing your staff to take 60+ minute training in one go, stop. It's ineffective and probably more damaging than doing nothing at all.

As an industry, do we want people to relate security to boring, laborious training? No, we want the opposite. We want people who are engaged and empowered to deal with security threats. Look at regular bite-sized learning materials, videos and games. Make the content about the individual and not your business. Focus on threats at home and you'll see people apply it in the workplace too.

I'm not going to bang-on about building a 'security culture' as I believe this can generate more problems. We should aim to make security a part of existing company cultures and this requires a tailored approach because every business is different.

## System patches, bug fixes, updates

The rate at which technology develops is often hard to follow at times. It has enabled organisations through digital transformation, but at a cost. As we strive for the latest technology, we often leave behind older systems and solutions. They may be in run-off or in the background running critical business processes. This has historically led to technical debt and the associated costs to maintain them. More importantly, these technologies are prone to receiving less security patches. We may also find the business enjoying their shiny new tech and forgetting what's hiding in the closet. You only have to look back to 2017 for the impact caused by WannaCry and NotPetya to the NHS and Maersk respectively.

The key takeaway here is that irrespective of the age of the system, security patches need to be applied within a reasonable timescale. The process should be foundational and embedded into day-to-day practice. I have first-hand experience of system patching and yes, it can get ugly. There are tools out there than can and will automate much of it. There are no excuses for not getting it right and IT resources need to be ring-fenced and made available.

## Policy

Nobody enjoys reading policy but there is a reason why it forms the backbone of security standards such as ISO 27001. Ultimately, it is about setting out the approach to security and boundaries for individuals to follow.

From a business perspective, policy is important as it's one area to lean back on when building a defensible position. Questions to ask yourself; can your policies be enforced? Are they simple and straightforward? Do you use layman terms and appropriate language? Can you reasonably expect staff to understand and abide by them?

## Process

Security should be embedded into business processes and not just a layer that is placed on top. This can only be achieved if security teams and officers embed themselves within the business. This can only be done if the time is taken to understand what the organisation does and how they do it. Naturally there are processes that are similar to all businesses. Starters and leavers is an obvious example here and highlights the interaction between security, HR, IT and managers across the business.

## Think twice before you sign the order for the latest vendor tech

Make sure you have covered the fundamentals before you engage with new security tech vendors. In most cases, you will already have the tools you need to achieve this. Before you make a case to purchase that shiny solution boasting AI capability, make a case to ring-fence IT resource to patch critical systems regularly.

Instead of buying a solution that protects you from 1% of known threats, focus on the human factor where larger percentages of security incidents and breaches are attributed to. There are other security fundamentals that I haven't touched on. These will feature in popular frameworks or standards (NIST, ISO 27001, Cyber Essentials as examples).

The technology driven world is exciting and continues to move at a phenomenal pace. We must remain grounded to ensure we don't lose sight of the fundamentals.

See More on Information Security Management Principles from TSG Training