When North Korea's hacking unit, nicknamed The Lazarus Group, broke into the national bank of Bangladesh in 2016, they had a whole range of hi-tech tools up their sleeves.

The country's elite cyber team was aiming to steal almost a billion dollars from the bank – money that would be used to prop up a regime which is under international sanctions. To penetrate its networks they used a bewildering variety of viruses with esoteric names like Macktruck, Nestegg and SierraCharlie.

But they knew that technical skill would only get them so far. To make sure that their viruses hit the right targets, at the right time, they had to understand the business they were targeting. Who works there? What departments are they in? Who controls the money? What hours do they work? What are the controls in place that might prevent us stealing the money – and how do we subvert them?

It was these insights into the bank's internal set-up that allowed the hackers in, and ultimately led to the theft of millions of dollars.

They targeted employees in the HR department with CVs containing hidden viruses. From there, they traversed the bank's computer network, and waited until the weekend (which runs from Friday to Saturday in Bangladesh) to start transferring the money. In the end, thanks to a series of mishaps, they only got away with $81m. But it was still a huge hit to the bank - and money it would never see again.

The hackers almost certainly didn't see themselves as business analysts. But the insight they gained into their target before they staged the raid has a lot in common with that industry. Getting under the skin of an institution and understanding how it ticks turns out to be a key skill for hackers, too.

There's a lot of scope for the BA community to be involved in security. For a start, most hackers would give their right arm to have access to the kind of information BAs hold on their laptops, phones and hard drives, because it would allow the crooks to target their victims much more effectively. As a result, BAs need to be aware of the risk they'll be targeted by hackers.

In addition, business analysts are often working at key moments of flux within an organisation – helping design the systems and processes that will guide its future. Hackers love those moments: all the usual procedures are disrupted, and that allows the cyber criminals room to manoeuvre, and potentially trick employees into clicking on links or downloading software that lets the hackers in.

Of course, not every BA wants to dive into cybersecurity – I'm sure that many feel they have enough on their plate already. But the good news is that having an eye to the cyber risk doesn't necessarily involve taking a bunch of courses and qualifications. Sometimes a change of mindset is enough. Put yourself in the role of a hacker – or any malicious individual – trying to break into your organisation; how would you subvert the systems and processes to get access, and once inside, to do some damage? Even if you don't have the skills or knowledge to implement protections, just identifying the risks might be enough to flag it up to someone elsewhere in the organisation who can.

In modern institutions, employees have unprecedented abilities – we can access tons of information and helpful systems at any hour, day or night, in an instant, from anywhere in the world. The flipside is that the hackers know this. They see every employee as a potential way in. Security is no longer the role of a discrete department – it's now a small part of all our jobs.