Cybersecurity is everyone's responsibility.

Imagine a customer walking into a store, accidentally falling due to a slippery surface or stumbling due to some obstruction. Who do you think in this situation is responsible for the accident? Is it the cleaner, staff, security guard, store manager, senior management, etc.? Who in your home is responsible for securing the doors, windows, or valuables? Take a moment to ponder this question - Who is responsible for cybersecurity?

The answer is that everyone has a responsibility to consider cybersecurity. Yet, as it has often been said, "everyone's responsibility is nobody's responsibility". With such a crucial area, we BAs must take that initiative. As business analysts, we interact and collaborate with business and technical teams and are best positioned to bring this topic to the table. As BAs, our job is to ask the right questions even if they are difficult and not miss any aspect to deliver a complete analysis. Hence it is imperative that we include cybersecurity as part of our analysis.

How do we do that? Tell me what comes to mind when you see or hear Cybersecurity. For example, a compliance team member might say, "it's about the compliance of cybersecurity laws, like, privacy". Somebody working in an IT team might say, "it is about securing the network or firewalls"; a system architect may say, "it is about securing the data and systems". And most business teams would say, "it's technical in nature, and hence the IT or the Cybersecurity team is responsible". If you were a business analyst, what would you say? Before you continue reading further, take a moment to ponder….what does Cybersecurity mean to you?

A few years back, I would have said the same as the business teams: Cybersecurity is the responsibility of the IT or the security teams, and I do not have to bother about it. And as a BA, eliciting and documenting my project's non-functional requirements was all I had to do until a personal experience fundamentally changed my perspective on Cybersecurity.

I was working on a customer subscription product some time back, and the data available for the subscription was the organisation's intellectual property. I was assigned an item which was at the bottom of a backlog. Note that the change was not a business priority and was at the bottom of the backlog. It was brought to my attention that the business and technical teams had already devised a solution for that problem. However, it still needed to be implemented because other items on the backlog had a higher priority. So as a good BA, I started to analyse the problem to get into the root cause of the issue and had conversations with the business, development and operations teams. The result of my analysis was shocking, as the root cause of the problem was a data breach. Even more startling was that the breach did not happen once but multiple times and the operational reports showed discrepancies due to the heavy data downloads, which was not a normal system behaviour, and nobody took notice and acted. Just imagine what would have happened if the entire data had been downloaded and freely available on the internet. What would impact the customers who paid for it, and most importantly, what would have happened to the organisation's reputation? Wouldn't the organisation cease to exist? **My crucial question was, why wasn't this a business priority?**

Why is this the case? Why are we not aware of Cybersecurity? What are we missing here?

Let's take a step back to gain perspective on the root causes of this issue affecting everyone professionally and personally. Understanding the background will help us evaluate why a focus change towards cybersecurity is necessary.

I started my career as a consultant analyst developer during the late 1990s. My job was to work with clients, understand their business requirements, design a database, build a system to meet their

business needs, prepare manuals and train users to use the new application. I was doing all of these things on a standalone computer. All my code, executables, operating system, and database, including the customer data, were in one physical system.

The only vulnerability apart from securing the physical equipment was using a floppy disk, which was used to copy data in and out of the computer. It could potentially corrupt the files if they contained a virus. Even if a virus corrupted a file, anti-virus software was available which could clean the data. This solution could be replicated on any other infected computers within the organisation. One solution for all computers.

Later, computers were connected as clients to servers, creating local and wide area networks. Today with the advent of the Internet and other technological advancements, systems are distributed across the globe. Imagine the potential weaknesses or vulnerabilities in a globally distributed system. What can go wrong in this new landscape? The list of potential vulnerabilities can become endless. There is no one solution to this current landscape. Unlike the earlier times when floppy disks were used, vulnerabilities in this new landscape come with their own risks and impacts.

Throughout my journey as a BA, I've adapted to the progressing technology and changing business needs. As the businesses started to expand, a shorter list of user or system requirements back then also began to develop into Functional Requirements (FRs) and Non–Functional Requirements (NFRs). Historically, security was considered an NFR. It involved who could and could not access a system or data relating to roles and permissions. Unfortunately, this approach falls short in the current situation. So the key takeaway message is that t**he more technology expands, the more vulnerable the ecosystem gets, and the more security controls are required**.

Business analysis enables organisations to see and understand the risks and make the right decisions, even if they are difficult. And if our analysis is incomplete and not all the risks are highlighted, the decisions made will obviously not be the right fit. Hence, as BAs, we are responsible for ensuring we deliver a complete analysis calling out every scenario that impacts cybersecurity.

A BA need not be a cybersecurity analyst whose responsibilities differ from a business analyst and focus more towards implementing controls to cybersecurity requirements. However, BAs need to be educated on the cybersecurity aspects required for the analysis and reach out to the cybersecurity experts as the project demands. There are multiple options for a BA to learn about cybersecurity. They can subscribe to cybersecurity content to learn more on the subject, obtain IIBA CCA certification, read the cybersecurity content on the IIBA website and attend BA and Infosec conferences to learn more.

About the author:

Bindu Chanaveerappa is the founder and director of I-Perceptions Consulting Limited, providing Business Analysis Services in the UK.

She is also a co-author of the IIBA CCA certification and a keen advocate for making cybersecurity inclusive within the mainstream business analysis. Bindu has taken this imperative message to several BA and Infosec conferences globally. Bindu and Terry Baresh, another co-author of the IIBA CCA certification, will be facilitating a workshop at BA & Beyond on the topic "Cybersecurity is everyone's responsibility".

Bindu is working on creating an online tutorial on "Cybersecurity for Business Analysts and project teams". She believes that every BA must be cybersecurity literate to deliver complete analysis. To know more, you can get connected with Bindu on LinkedIn.