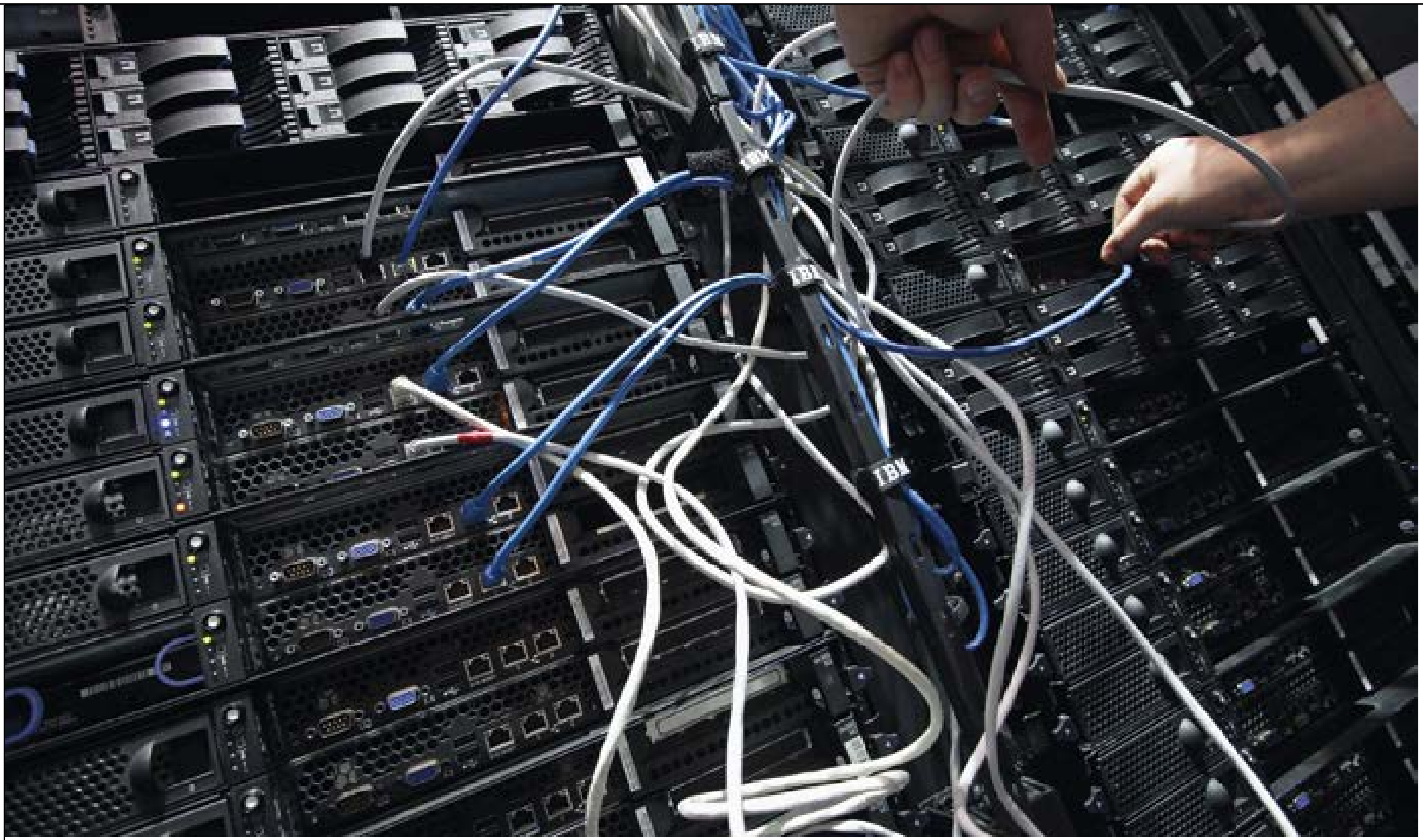


Soft skills are just as important for the security architect as technical know-how

Picture credit: Getty

SECRETS TO SECURITY ARCHITECT SUCCESS

Cristian Bojinca *reveals the key skills required by the IT industry to ensure a robust infrastructure*

The security architect job is a well-established role in the IT industry. Security architects normally focus on the measures that are required to protect the enterprise from threats by securing the corporate networks and their core systems but also defining an appropriate security-level classification for information technology assets, security architecture principles and policies that will provide the foundation for one of the important responsibilities of a security architect, namely governance.

Most companies have implemented security controls or checkpoints to ensure the other domain architectures are in line with security principles and policies. Any new applications, systems and infrastructure must ensure the security rules are baked into the architecture so that the systems not only do what the business wants to do, but that they are also secure enough to avoid being hacked by the most junior hackers. So anybody would expect the company to hire security architects to define these policies and provide governance for the projects or initiatives under way.

The role seems to be quite straightforward and requires the individual to have a lot of depth into the security concepts including (but not limited to) protocols, vulnerability assessments, authentication and authorisation mechanisms, encryption, *etc*. and be able to provide the governance acting as a central point of contact for security requests including consulting on projects, work with domain architects to ensure security policies and controls are implemented. All these jobs will mostly list the technical competencies and certifications the successful candidate must have to even sit down for an interview. But the main question one should ask is: are these enough to have an individual successfully perform the job?

SECRET INGREDIENTS

In this article we will discuss the secret ingredients that differentiates the successful security architects from those that fall short. We will reveal how focusing your attention to other areas of your professional personality will make a huge difference in the day-to-day job.

Although a security architect is supposed to be a specialist in IT security, they differentiate from other IT security professionals (such as security administrators) by having a T-shape personality and combing deep expertise in security areas with broad experience and knowledge across the IT industry. The security architect is supposed to collaborate with other domain architects (such as application, infrastructure, data, system, solution, *etc*. architects) to ensure the security controls are enforced. How will they do that if they do not have the minimal depth required to understand what domain architects are talking about? To be clear, this is not about being a specialist in application, infrastructure, data, *etc*. architecture, but being able to have the minimal knowledge required to understand what the security aspects of a specific application technology are and how they can relate to the security policies. If you are using an application container, how can security services (such as authentication, authorisation) provided by the container satisfy the security requirements? If you are not able to understand the domain architecture basic terms then how can you work together with the domain architect to ensure they build the correct architecture from the security point of view? As a security architect you are supposed to provide security governance being able to vet the solutions and ensure they are in line with enterprise security principles and policies.

THE SECURITY ARCHITECT FREQUENTLY INTRODUCES CHANGES THAT AFFECT THE WHOLE ORGANISATION

Second but maybe sometimes the most important ingredient is actually a mix of ingredients called soft or performance skills. The name comes from the fact they constitute the set of behaviours or actions that need to be performed successfully within a particular context to achieve the best outcomes. These include:

- **Leadership** – often mistakenly considered something for managers only, leadership is an important skill the security architect should demonstrate by establishing trust with the important stakeholders, never imposing leadership, but getting things done through personal influence (backed by solid technical knowledge) and credibility. In order to be able to effectively lead, the security architect needs to be able to build relationships with the most important stakeholders and establish trust. Without this the architect will not be able to do their job effectively no matter how proficient they are on the technical side.

Leadership might apply to both leading a team of IT security professionals, but also to providing leadership to other domain architects that will look at the security architect as the ultimate authority in the security domain.

- **Communication** – defined as the activity of conveying information is extremely important for the security architect. No matter how well you might know the network of the organisation and ensure it is well protected against external attacks without the ability to effectively communicate this vision to the other domain architects and IT security professionals this compelling vision might never be implemented. To maximise the security architecture benefits for the organisation the security architect must be able to follow up with the implementation of their vision and be able to communicate the details to the project team members and other stakeholders. Communication also implies listening and a good security architect will need to first and foremost listen to domain architects and other stakeholders to ensure they understand the organisation specifics of the IT ecosystem.

IT'S GOOD TO TALK

Sometimes the architect might need to use communication skills to negotiate conflicts instead of leaving things bubbling under the surface until an explosion occurs.

- **Presentation** – this is another soft skill I cannot emphasise enough how important it is to be successful as a security architect. As any other architect, the security one has to be able to deliver effective and engaging presentations to a variety of audiences. Presenting to the executives/management requires a totally different way of organising the information than presenting in front of domain architects that have a minimal technical depth in security or presenting to IT security practitioners for which security is their bread and butter. For all these different audiences, the security architect must be able to create and deliver a clear, concise and compelling presentation. Again, no matter how good you are with the technical concepts of the security domain (as you would most likely have a security administrator background), without good presentation skills you will not be able to make others understand your security solution so they can properly implement it in their domain architecture.
- **Stakeholder management** – another important aspect of the soft side of the security architect. The human aspect of the security transformation is usually the one that makes the difference between success and failure. Most important stakeholders must be identified early in the project and their input must be used to shape the security architecture.

This means ensuring you have not only the support of the executive/management stakeholders – as they understand how to change the security ecosystem – but also the support of the domain architects and IT security practitioners who understand how the new architecture will better serve the enterprise and protect the organisation.

- **Change management** – defined as the approach to shifting or transitioning from current to future state, this is also an important soft skill for security architects. Although they will not (most likely) act as a change manager, due to the nature of the architecture job and the fact that most of the time architecture means change, the security architect should be able to fully understand change management frameworks and how to react in each phase of the change to ensure its success. The security architect is most of the time the one introducing changes that affect the whole organisation (such as data classification, network security zones, applying security principles such as least privilege or deny by default).

LEADERSHIP IS AN IMPORTANT SKILL THE SECURITY ARCHITECT SHOULD DEMONSTRATE

The security architect should be able to get support from the sponsor of the specific change, as the main cause of failed changes is the lack of this kind of support. When you come up with specific security reference architecture and start implementing it, if the sponsor is not actively supporting the change the others will not pay attention and most of the time they will revert to the old ways of doing things. Most of the time, the IT practitioners expect from the security architect to coach them through the change in order to understand, implement and reinforce it.

- **Consulting skills** – last but not least, the successful candidate must demonstrate consulting skills advisory skills, consensus building, effective client relationship, effective communication and provision of excellent client service. There is a preconception that only the external consultants must have consulting skills, but as a security architect being proficient in consulting makes a huge difference in building relationships with the stakeholder and being able to navigate the treacherous seas of 'architecture politics'.

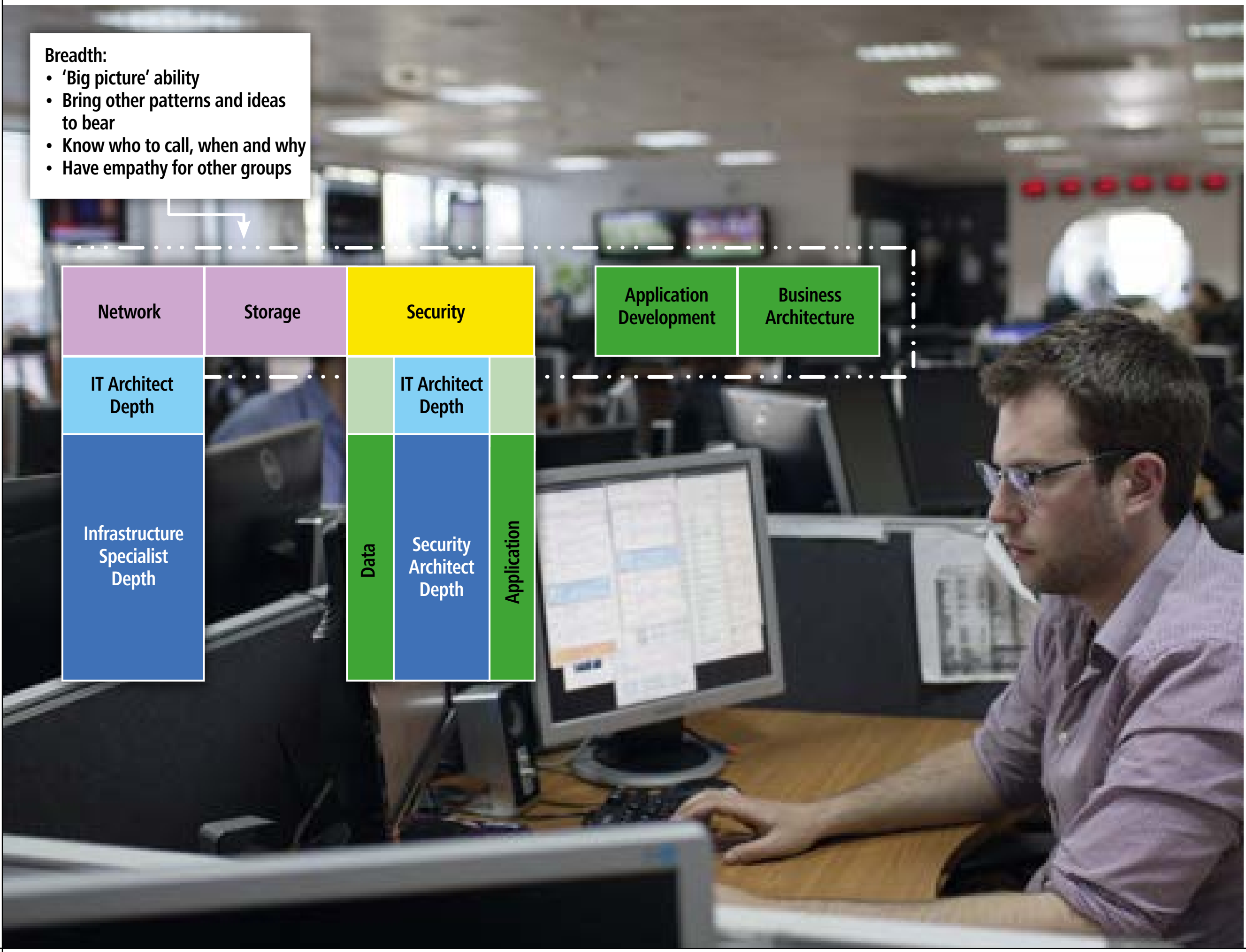
Security architects also act as consultants and need to be able to connect with domain architects to help them shape the domain architecture solution from the security point of view.

Being proficient in other soft skills (such as communication, negotiation, presentation, planning, *etc.*) will definitely help you to have a successful consulting engagement model.

Being proficient in these (and many other soft kills) will definitely help you become a more well-rounded security architect, able to not only create the security solution, but also be able to communicate it to the stakeholders and lead them to a successful implementation. This will greatly increase your chances of being in demand as people always want to work with IT practitioners that have a human side as well ●

Cristian Bojinca is an enterprise/solution architect specialising in setting up architecture practice by identifying specific IT architect roles and tailoring architecture frameworks for the needs of the organisation. He recently wrote *How To Become An IT Architect,* published by Artech House.

The 'T-Shape' personality is believed to fulfil the most important roles for security architects



Picture credit: Getty