

Introduction

Nobody would deny that our industry is dynamic. In fact, it takes a constant effort to stay on top of the changes. Unfortunately, most security professionals are so focused on the tasks at hand that it's hard to follow the subtle changes in the way companies are redefining "classic" security roles. I've been fortunate as a recruiter who sits in on numerous calls with clients to take note of the subtle and not-so-subtle ways companies are redefining classic security roles and responsibilities. Let's look at two roles—the Security Engineer and Security Architect—and see how they have changed over the last decade.

The Security Engineer

Once upon a time, when a client was hiring for a "security engineer," they were almost always looking for someone with a focus on network security and security administration. Basically, if you had a strong understanding of network protocols, knew how to harden an OS, worked with firewalls, and knew how to scan for vulnerabilities, you were good to go—and for a while you could almost name your price. Well, those days are long gone. Now the role of security engineer is much broader and harder to define, with numerous areas of specialization like identity and access management, vulnerability management, and application security, to name a few. Now companies are looking for people who have deep technical backgrounds as well as appropriate levels of risk acceptance, so effective and measured security controls can be developed. The next generation of security engineers is really best described as hybrids of hard-core "geeks" and business analysts. For some this is a nightmare; for others this adds new dimensions to the job and requires advanced levels of creative problem solving. Regardless, this is the direction where corporate security engineering roles are going, and to ignore the changes is to risk commoditization.

The Security Architect

A similar change is occurring with how companies define "security architects." In the past, security architects were responsible for designing security infrastructure and developing the policies and procedures that defined their use. While these are still core parts of the job, the clients I've been working with are looking for security architects who are capable of doing more. Part of this change is due to the constant introduction of new regulatory requirements and industry standards. Security architects must not only ensure that the solutions they're designing work from a technical standpoint, they must also meet regulatory and compliance objectives. This means that security architects have been forced to become subject matter experts on the host of regulatory requirements related to their industries. Security architects are also tasked with providing subject matter expertise on projects that span their organization, because virtually every project has an IT component. Therefore, security architects require the interpersonal and project management skills necessary to be effective internal consultants. This is especially true when more and more companies are promoting a culture in which security is not allowed to say no to the business. Security architects have to understand all of the risks of a given project as well as the risk tolerance of their internal client, and then develop solutions that bridge that gap. To do so requires a clear understanding of the business that's being supported, the ability to collaborate with non-technical people, and the judgment to know when and how to take a stand

on security matters that can't be sidestepped.

Conclusion

For the purpose of this article I chose the Security Engineer and Security Architect positions because they represent classic security roles that have evolved considerably over the last decade. The same can be said for just about every other position or title in our industry. Books have been written about the evolution of the CISO. Application development is being revolutionized by the introduction of security requirements. Business continuity professionals are taking more proactive roles as organizations look at security from the broader context of Operational Risk Management. And naturally, recruiters serving our industry have been forced to elevate their understanding of how our field is evolving so they can more effectively serve their clients. It's well established that Information Security is made of three major components—people, process and technology. In the past, it was common for security professionals to concentrate heavily on one of these three areas. This isn't the case anymore. As a career-minded security professional, it's more important than ever to develop capabilities that span the trinity of people, process and technology.

Jeff Combs has been a recruiter with Alta Associates since 1999.