

Entry-Level Security Technician: Laying the Groundwork

DEANNA HARTLEY

A well-choreographed play undoubtedly has some dedicated behind-the-scenes personnel contributing greatly to the success of the project.

In the world of IT security, entry-level security technicians fit that profile.

Entry-level security technicians are required to do a lot of grunt work such as coding, but they also get opportunities to do some hands-on work — usually under the supervision of a senior colleague.

People in this job role at [Laurus Technologies](#), an IT solutions company, delve into a great deal of research from a pre-sales standpoint, said Brian Wolfe, president and partner for security and compliance solutions at Laurus.

While it's typically the more senior professionals who meet with clients and sales teams to identify the requirements and business drivers for projects, research and prototyping are entrusted to entry-level security technicians. Once a sale is finalized, these professionals have the opportunity to do hands-on work under the direction of their senior colleagues, including preparing an environment for the installation of software and undertaking the installation and customization.

Broad-Based Functions

At Laurus, entry-level security technicians work on one of two assignments: data-loss prevention (DLP) and identity management (IdM).

DLP systems monitor all the Internet traffic entering and leaving the network and identify the dialogues, conversations and applications running. These systems help identify any vital or confidential information the organization doesn't want to leak. For example, health care organizations want to keep patient health records private, or commercial companies want to ensure Social Security numbers remain unseen.

The service Laurus provides its customers is known as an exposure assessment, and this is where the entry-

level security technician comes in. He or she will insert the DLP system into the network — typically working with the network administrator — and will be responsible for working with senior counterparts to compile all the information into a report.

"[They translate] a lot of what looks like meaningless data into something you can relate back to HIPAA (Health Insurance Portability and Accountability Act) or SOX (Sarbanes-Oxley Act) compliance violations — the regulatory types of violations that these conversations correspond to," Wolfe said.

The demand for IT security professionals is growing, and those hoping to make it in the field will need good technical skills and a solid business background.

Entry-level security technicians at Laurus also work on identity management. IdM refers to the maintenance of online usernames and passwords — IDs — and typically comes into play when new employees are hired or on-boarded. Responsibilities include solving problems related to password management, password synchronization and user self-service. Entry-level security technicians get involved in these projects by doing a lot of the workflow coding.

All IdM products used by the company have workflow engines, and there are various kinds of forms that need to be customized to match the customer's business process. Entry-level security technicians work on the forms and the programming behind the forms.

"Entry-level technicians are not designing this stuff; they're not the ones gathering the requirements from the customer. But typically they'd be sitting in on the discovery session," Wolfe said. Sometimes they are assigned parts of the documentation to work on, but typically they undertake the bulk of the coding.

Technical Training

So what type of training or technical skill sets does this job role call for?

According to Wolfe, many entry-level security technicians who work on DLP have a background in networking and systems — perhaps a Windows administrator background. These technicians work on projects that don't require a lot of skills related to application development. But sometimes they work on single sign-on or enterprise single sign-on projects that are less coding-intensive.

Wolfe said an entry-level security technician likely will benefit from certifications such as the [Microsoft Certified Systems Engineer \(MCSE\)](#) and [Cisco Certified Network Associate \(CCNA\)](#), or the [Cisco Certified Network Professional \(CCNP\)](#) for those interested in DLP work.

"The reality is that [entry-level people] have to undergo a lot of training before they ever get on

projects, [and] we're really not expecting to see that they've had experience or training on some of the products we deploy," Wolfe said.

On the other hand, security technicians who work primarily on IdM projects usually have a background in applications development. Because most of the products on the identity side are Java-based, having some type of Java development experience is a strong technical requirement. A handful of the Microsoft products are .NET-based, so a foundation in that is useful.

It's not uncommon for entry-level security technicians at Laurus to have undergraduate degrees in computer science. But Wolfe's advice for people looking to step into this job role is to combine a computer science or similar degree with some type of business credential. An ideal candidate would have a bachelor's in computer science and an MBA, or vice versa, he said.



Learning about the business aspect is important, Wolfe said, because the requirements of security are mapped to the regulatory requirements, such as SOX compliance generally, Gramm-Leach-Bliley Act compliance in the financial sector or HIPAA compliance in the health care industry.

It's important for security technicians to have an understanding of how businesses are organized so they know what is and isn't appropriate data for people to be allowed access to.

Entry-level security technicians are required to do a lot of grunt work such as coding, but they do get opportunities to do some hands-on work – usually under the supervision of a senior colleague.

"If you just have an applications development background, then there are roles we have that people can add a lot of value for us. But by having an understanding of the business side, people have a much better ability to go in and be more consultative," Wolfe said.

For instance, a security technician might work with customers to perform an IdM road map and assessment. To do this, it is imperative to understand how the business operates and to be well-versed in some of the processes associated with it, such as on- and off-boarding.

Nontechnical Requirements

Though nontechnical skills — specifically soft skills — always are an invaluable asset, Wolfe said they're not a prerequisite for undertaking certain projects.

For instance, typically, a team of five to seven people will work on larger projects.

"If [a person's] English communication skills aren't really solid but they're technically very sound, we can still have [that person] add value on those larger projects because our people will manage them and they'll be the technology experts," Wolfe said. "We've had people who are real superstars with the technology, but

we can't have them on a project by themselves, [so] it depends on the types of projects [they are assigned]."

On smaller, one- to two-person projects, soft skills are a must. "On projects like that, having good communication skills [and] interpersonal skills is an absolute requirement because there's nowhere to hide," Wolfe said.

Additionally, entry-level security employees looking to advance into management and take on more responsibility must have good communication skills — and that doesn't just mean talking to colleagues. They should be able to interact with and present to both customers and executives.

"As they progress, if they have [good] communication skills, they might start to do design work and get involved in the discovery sessions we do with customers in pre-sale," Wolfe said. "Once they've got a couple of projects under their belt and they've demonstrated that they've mastered the work for certain types of projects, we might give them a chance to run a project."

At Laurus, the next step up would be a project leader position and then a practice lead, which is a person who oversees projects and performs the design and estimation with a handful of people reporting to him or her. The next role would be that of a practice manager, who would be in charge of a number of practice leads.

Future Prospects

On a bright note, the market seems to point to a need for more professionals in the IT security field, Wolfe said.

"[Issues surrounding] security are only getting more complicated," he said, noting that regulation was a significant talking point during the 2008 U.S. presidential race.

"[It] always ends up boiling down to more things on audits [that] people are going to be looking for, and that will translate to more experts needed to go in and assess whether the security program or the way security is being implemented in an organization is in compliance with the regulation," he said.

Further, the fear of outsourcing is low in IT security, as it is difficult to outsource these jobs to Asia or anywhere else, Wolfe said. ☺

— Deanna Hartley, dhartley@certmag.com