CSO
FROM IDG

CAREER TRACKER

What it takes to become a **security architect**

What it takes to be a security architect

While the path to security architect varies, anyone considering the role should have a passion for IT infrastructure and protecting data.

BY BOB VIOLINO

Security architects are the people responsible for maintaining the security of their organizations' computer systems, and as such they must be able to think as hackers do in order to anticipate the tactics attackers can use to gain unauthorized access to those systems, according to the InfoSec Institute.

Anyone in this position can expect to have to work odd hours on occasion, and needs to be constantly up to date on the latest security threats and available tools.

Sometimes people who ultimately take on the role of security architect, like Jerod Brennen, could not have predicted such a career direction when they were younger. When Brennen began attending Capital University, a small liberal arts college in Ohio, in the 1990s, he intended to pursue a career in the film industry as a composer.

Computer-generated music was an emerging industry at the time, so he started as a computer science/music composition double major. Some of the technology classes were not to his liking, so he quickly dropped the computer science major and focused on getting a degree in music education.

"It wasn't until my student teaching experience my senior year that I realized teaching in the public schools wasn't my cup of tea, either," Brennen says. "I spent a bit of time after school jumping from job to job, but when my wife and I decided to start a family, I decided to revisit my love of tech and computers to see if there was a career path I could pursue. Turns out if you're willing to dive in and learn from the ground up, you can find the opportunity you're looking for."

While working as a hardware technician at Rent-a-Computer from 1999 to 2000, Brennen's job was to build computers from scratch and set up systems and local networks for training classes.

Next he worked at Sterling Commerce's call center as a solutions support specialist, first on a contractor basis and then full time. His job was to provide software support for Sterling's electronic data interchange customers.

In 2001 Brennen joined power company American Electric Power (AEP), and after some time at the company responded to an internal posting for an information security position that needed someone with UNIX experience, which he had. While at AEP he earned a CISSP.

A big opportunity arrived in 2006 when a recruiter called about a newly created information security role at retailer Abercrombie & Fitch, and

Brennen was hired as manager of information security.

"Even though I was a full-time infosec pro at AEP, I was pigeon-holed," Brennen says. "I wanted to do more." Abercrombie needed someone to come in and build out an information security program that supported its Payment Card Industry (PCI) compliance efforts.

"I had no management experience, no credit card security experience and no retail experience," Brennen says. "But I threw my hat in the ring anyway." He spent the next four years building the security program from the ground up.

Initially he had no budget and no team, just time, local administration rights and whatever free or open source tools he could get his hands on. "I spent the first few months taking on every project and adopting every security tool I could," Brennen says. "It didn't take long before I had more on my plate than I could possibly handle alone."

Brennen was demonstrating value, though, and was able to justify expanding the team to four staffers supported by 20 representatives from throughout the company. The team deployed a security framework that aligned with the company's operating model.

"That's when things really clicked," Brennen says. "By the end of my time there, we were supporting 12 enterprise-level security tools including a robust identity and access management implementation with a global user base. We were staying on top of our internal audit and external compliance obligations, and most importantly, we were protecting the personal information of tens of thousands of employees and customers who didn't even know we existed."

Other positions followed, including stints as CTO and principal security consultant at risk management company Jacadis, and associate director at Ohio State University (OSU).

At Jacadis, Brennen helped clients identify and implement the security controls, and conducted risk assessments and security program reviews. "I worked on projects ranging from IT takeovers for small, not-for-profits to application source code security reviews for large federal clients," he says. "The really rewarding part, though, was that I was able to apply my enterprise experience in helping our clients build their own security programs."

At OSU, Brennen built and managed a risk management program. From there, he moved to his current position

> **"The really rewarding part, though, was that I was able to apply my enterprise experience in helping our clients build their own security programs."**
>
> -**JEROD BRENNEN**, SECURITY ARCHITECT AT GBQ PARTNERS

CAREER PROFILE

Security architect

Certifications	Certified Information Security Manager (CISM) or Certified Information Security Professional (CISSP)
Potential employers	Any business with a large IT infrastructure that must secure company, employee and customer data
National median salary	$109,794 (according to Payscale)

as security architect at GBQ Partners in February 2017. GBQ is an accounting firm with audit, tax, and advisory services in six cities.

"As much as I loved the risk management work I was doing at OSU, the decision was a no-brainer," Brennen says. "I'm back to architecting security services that will help our clients. I'm back to building."

While working at Jacadis, Brennen developed a security framework that "gets away from the hundreds of detailed controls that organizations should implement and focuses instead on the basic blocking and tackling," he says. "My goal here at GBQ is to expose more and more organizations to that framework and to help them build a solid foundation in information security."

More important, though, Brennen wants to help clients "build out information security programs that enable them to get back to the core mission of their business, whatever that mission might be."

Another security architect, Jerry Magginnis, also didn't start out planning a career in the field. Magginnis majored in both statistics and market research at Purdue University, where he received a bachelor of science degree in industrial management, and wanted to pursue a career in marketing research.

The first company he worked for out of college was advertising firm McCann-Erickson Worldwide, where he worked a variety of positions including associate director of consumer research, account executive, MIS manager, communications director; telecommunications director, and global telecommunications director.

He left the company in 1998, joining utility Louisville Gas & Electric as technical consultant. Following that Magginnis moved to healthcare company Kindred Healthcare, where he took on his first security-related position as senior security analyst.

In 2005 he joined BMW Financial Services, where he was senior application security architect. Next came a five-year stint at Abercrombie & Fitch, where he served as security architect and worked with Brennen.

Magginnis joined healthcare company Cardinal Health in 2010 and worked there for three years as senior security architect. In 2013 he joined his current employer, home security products company ADT Security Services, as IT security architect.

"My background in each of the positions I held expanded my capabilities for the next opportunity," Magginnis says. "I pushed myself to learn beyond the assigned job requirements into areas that augmented my role. I read a lot of books, did the hands-on work I assigned to my direct reports to understand what they went through daily, and I took courses for certifications."

Once Magginnis got well into information security as a career, he was always being sought out by recruiters. "I have never been without a job," he says. "I also made a point to never pass up an offer to interview for a position at another firm that promised to improve my career."

Each company had technologies Magginnis was not comfortably familiar with, so he signed up for vendor classes and read all their materials. "A CISSP is a hard requirement for this field; [I'm] glad I got mine in 2001," he says. "It opened up a lot of doors in subsequent years."

His plan is to retire from his current employer. "I have already started a gourmet pizzeria and meadery that will be my 'hobbies' in the foreseeable future," Magginnis says. ■