Data breaches are costly – in revenue and reputation – and organizations are actively looking for talented professionals who can help protect their data stores. See what issues are keeping CIOs up at night and the career opportunities available in this growing field.

Data security has become an urgent priority for business. Boards of directors have finally realized that without highly skilled cybersecurity expertise on staff, their organizations face increased risk, unbudgeted expense and potential damage to their corporate reputations. Management in both the public and private sector are scrambling to bring on staff that can help ensure the integrity of their computer systems and data stores.

As a result, data security talent is highly prized, whether in the field of finance, healthcare, government, education, national defense, retail or any of many other major industrial segments. And reflecting the overall state of cyber security employment, demand far outstrips supply.

As an example, a report by the Bureau of Labor Statistics found that the role of security analyst is expected to grow by 18 percent by 2024, compared to an overall job growth rate of seven percent. Yet that sounds downright conservative compared to the projection made by U.S. News and World Report, which reported that the profession is growing at the rate of 36.5 percent through 2022. Similarly, IT security was named the third most in-demand skill for the next year by Computerworld in its IT Salary Survey 2016 Results.

Although crossover exists between data security and systems or network security, what distinguishes the former is its oversight of specific areas of IT operations: information leakage, privacy considerations, access control, data encryption and shared computing infrastructure.
TRENDS DRIVING DATA SECURITY OPPORTUNITIES

Early in his career, says Randy Marchany, long-time chief information security officer for Virginia Polytechnic Institute and State University, much of the emphasis for cyber security and its training practices was on understanding how computer systems could be broken into and taken over. Now the attention is on protecting data and preventing others from stealing it. As he explains, “With all the major data breaches that have happened, a lot of what we’re trying to help students learn is how people can get to the data and how to design the defense against those types of attacks.”

As the number of cyberattacks increases, Marchany adds, so do the responsibilities taken on by people handling data security. Just as cyber criminals are relentlessly trying out new methods to get inside corporate systems, so must the security professionals in charge of protecting the data on those systems continually adapt to stay ahead of the bad guys.

It’s that ever-changing variety in his own job that keeps Marchany inspired. “The university has aspects of a small town. We have a police department. We have transportation — buses running through campus. We have hotel lodging in the form of dorms. We have a power plant on the university that supplies power to the university as well as shares power with the local electrical utility in town. So there are cyber security issues for a whole wide range of things. I may do financial security one day. Then I may do engineering security another time.”

Marchany, who is also a member of the faculty for Virginia Tech’s Online Master of Information Technology and heads up the university’s innovative Information Technology Security Laboratory, points to several trends driving up demand for people who can protect their companies’ data assets.

**Security fundamentals haven’t gone out of style.** As managed security service provider NTT Security stated in its Global Threat Intelligence Report for 2015, more than three-quarters (76 percent) of identified vulnerabilities turned out to be at least two years old — a sure sign that organizations need to make sure they get the basics — such as staying on top of system patches — right.

**Phishing is making a comeback.** It used to be easy for the informed email user to recognize fake emails. Bad spelling, poor grammar and odd formatting were clues indicating trouble. No more. “Spear phishing” — targeted attacks — provide just enough personalized information to convince the email recipient that the link embedded in the message is legitimate and that his or her password does need changing.

**Effective security policies are collaborative.** Organizations that develop their security processes in isolation face an uphill battle in getting users to adopt them. What’s needed is continual “consultation,” as Gartner advises, to draft a “sustainable” set of policies that make sense in the realm where people are trying to get their jobs done. It isn’t necessarily the most security-
knowledgeable person who should develop the policies, but the one with a communicator’s touch.

**Data breaches will happen; the smart companies are the ones prepared to respond.** If well-protected JP Morgan Chase, Target, eBay and Anthem can suffer the ignominy of cyber break-ins, so can any other operation in the country. What will distinguish leaders from losers is the robustness of their processes for dealing with break-ins and theft. That same NTT Security analysis found that 74 percent of organizations lack formal incident response plans.

**Staying informed is job one.** As American corporations are increasingly pressured to share data with federal agencies and government officials in the European Union and the United States wrangle with privacy protections, new laws and border agreements are surfacing that govern the handling of personal data. Security professionals who excel will be those who know how to stay on top of evolving privacy regulations.

Becoming a well-rounded data security expert isn’t simply about “learning how to hack a machine. It’s not just learning how to defend against a machine. You have to know how to do policy. You have to know what the laws are,” Marchany points out. Plus, you need a bit of hands-on experience with security utilities as well.

“I’m expecting that most of these online masters students will be managers or supervisors,” he explains. “But I want them to have exposure to some of the tools that their technical staff might be using, so they’re familiar with it.”

As Marchany observes, it’s the combination of hard skills and soft skills that make up the complete package. “I can be the most technically competent CISO in the world, but if I can’t frame my arguments to my upper management in a language they understand, then I’m worthless.” Combining the technology of cybersecurity with the business of IT, he believes, is what really sets up people for success in the data security field.

Yet, no matter how compelling the employment opportunities are, the work tends to exact one unique burden on data security professionals that few others face, warns Marchany. They come out of their training “totally paranoid about all of the technology that they’re using — smartphones, laptops, internet of things devices.” They understand things the rest of us just don’t.
AN UNCONVENTIONAL HIRE

As companies vie to hire data security professionals, they're not simply considering candidates with a deep IT resume. That's good news for anybody coming from a non-traditional background.

In fact, says Randy Marchany, certain non-IT skills stand out as essential for anybody seeking a role in data security. One example is the ability “to communicate to people that they need to be careful with their data and careful with their devices and put it in a way that means something to them — that’s a more valuable skill than just about any other in data security.”

Marchany has also noticed that people who are good at solving crossword puzzles show a real aptitude for data security because “they can extrapolate words out of a couple of snippets of information.” That ability “to take a few pieces of data and come up with possible theories as to what is going on,” he notes, is a “really useful skill” to have.

Those able to “speak business” also have a definite advantage when going after a management position, Marchany explains. “Putting a cyber threat in terms of risk — How much would this cost the company? What about income loss? What happens if the intellectual property for our signature product is stolen and a competitor builds it for much cheaper? — will enable them to speak to the executives of the organization in the language they understand.”

Virginia Tech’s Online Master of Information Technology has been ranked number two in the nation by U.S. News & World Report for best online graduate computer IT programs. Learn more here.