Big Data, Big Security

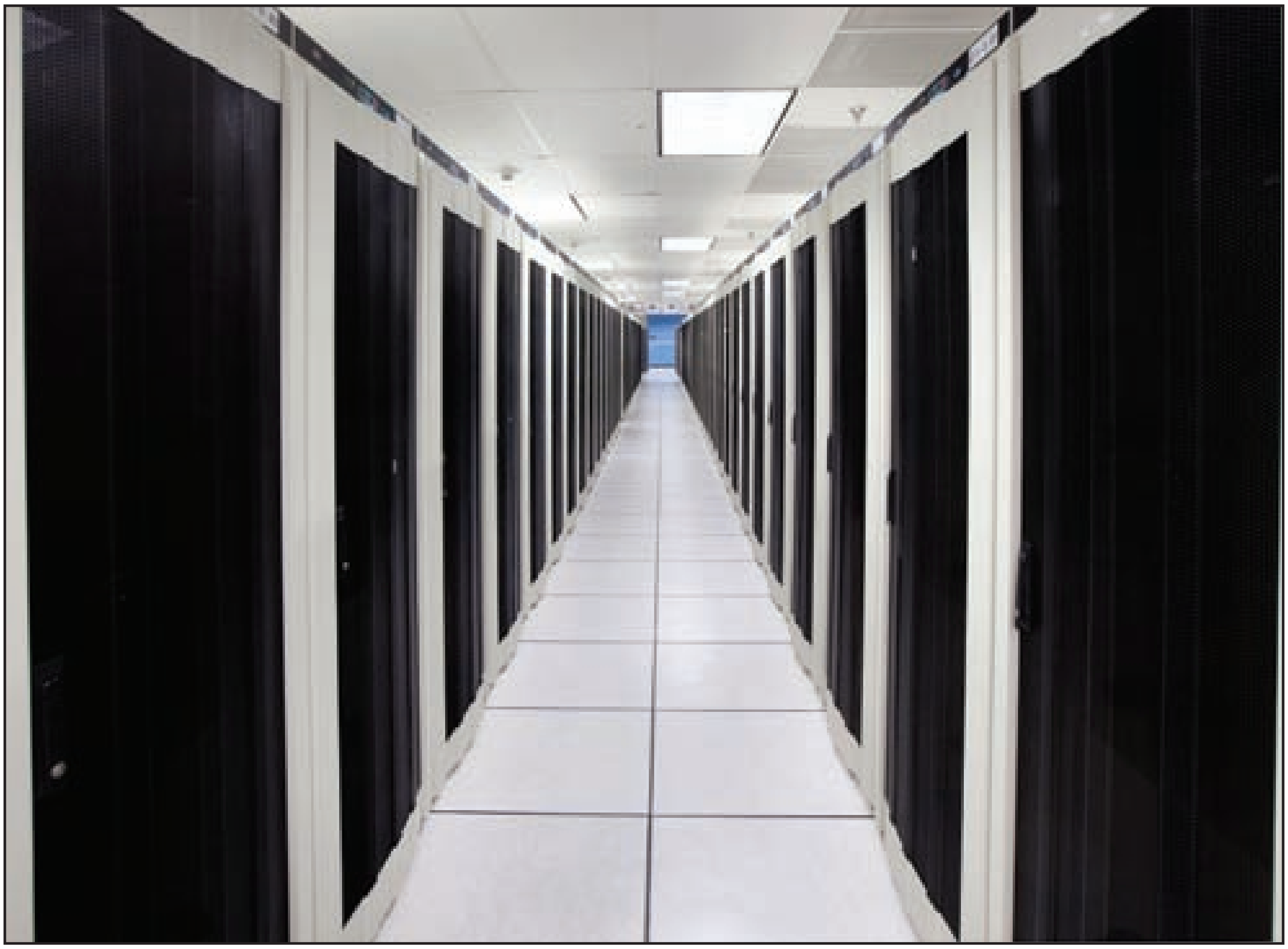
By Diane Ritchey, Editor

Heartland Payment Systems, TJX, Epsilon and Sony: what do they have in common?

For one, trouble with the data center. Heartland Payment Systems, a payment processor based in Princeton, N.J., was the victim of a major cyber attack in 2008. Criminals installed spying softwar e on the company's computer network and stole the numbers of as many as 100 million cr edit and debit car ds. TJX, the F ramingham, Mass., retailer that o wns national chains including TJ Maxx and Marshalls, estimated that a 2007 data br each would cost the company about $25 million. But in the end, the total cost was at least 10 times as high.

At Retirement Systems of Alabama, no one gains entry into the data center without complete background checks, current credentials, turnstiles with a biometric credential and additional biometric readers to get you to the next step.

In March 2011, hackers stole millions of names and e-mail addr esses from the Dallas-based marketing firm. E psilon handles e-mail lists for major retailers and banks like Best Buy, JPMorgan, TiVo, Walgreen and Kroger. A study b y CyberFactors, a



Securing a data center goes beyond the IT infrastructure. Physical security plays a major role, as well. Physical access to the site is usually restricted to selected personnel, with controls including bollards and mantraps.

cyber risk analytics company, estimates that the breach could cost between $225 million and $4 billion.

The Sony data breach, which exposed information from more than 100 million user accounts in April, could prove to be the mostly costly data breach of all time. Hackers obtained personal information, including credit, debit and bank account numbers in some instances, of PlayStation Network users and Sony Online Entertainment users. After discovering there had been a breach, Sony shut down both networks temporarily. The Ponemon Institute estimates that the breach could cost Sony and credit card issuers up to a total of $2 billion.

The losses and risks are even troubling, given the potential growth that data centers seem to indicate. Despite growing concerns of a global economic slowdown, the companies that construct and operate data centers expect growth next year to match levels last seen in the world economy's boom years: about 19 per cent. The growth of cloud computing is prompting increased demand for data center space in North America, according to a survey by Digital Realty. The growing interest in cloud adoption, along with the resumption of planned expansions that were deferred due to the economy, suggests robust growth ahead for the U.S. data center industry, the report says.

In addition, 92 per cent of IT decision makers at large companies said they will "definitely or probably" expand their data center footprint in 2012, the highest number in the six-year history of the survey by Digital Realty, which is the largest operator of data center facilities. By comparison, 70 percent of respondents said they had expanded their data center operations over the past two years.

Securing the Data

Yet there are many success stories of data secured successfully. Take, for example, Silver Cross Hospital's recently opened data center. The hospital recently opened a 600,000-square-foot, $370 million medical complex with an outpatient center, medical service building and hospital in New Lenox, Ill. The project also included a new 2,450-square-foot data center, 50 per cent larger than its existing one.

Even more – OSF HealthCare's new Children's Hospital of Illinois in Peoria and the soon-to-open Ann & Robert H. Lurie Children's Hospital of Chicago – have combined new data centers with new medical facilities. The hospitals are establishing a technology foundation for healthcare that will be dominated by electronic health records that cannot be compromised.

In addition, Cook County Health and Hospitals System (CCHHS) of Cook County, Ill., have deployed a unified virtual data center infrastructure, worth nearly $3 million, to serve the operational needs of some two dozen facilities across the Chicagoland area. The CCHHS cloud solution reportedly speeds up access to patient care data for clinicians and staff personnel while giving the CCHHS a data center infrastructure that is ready for future growth.

"At a data center, it's all about anonymity," says William Holmes, head of critical infrastructure and facilities for Bytegard, a holdings company that acquires, develops and operates wholesale data center facilities.

Beyond new construction, securing a data center's IT infrastructure, physical security also plays a large role with data centers. Physical access to the site is usually restricted to selected personnel, with controls including bollards and mantraps. Video camera surveillance and permanent security guards are almost always present if the data center is large or contains sensitive information on any of the systems within. The use of finger print recognition man traps is starting to be commonplace.

"At a data center, it's all about anonymity," says William Holmes, head of critical infrastructure and facilities for Bytegard, a holdings company that acquires, develops and operates wholesale data center facilities. The company recently acquired a new 214,000-square-foot data center in downtown Silver Spring, Md. It is the largest multi-tenant data center in the state of Maryland. The facility is rated ultra-secure for government interests, and it is also considered "financial grade" and home to one of the world's 10 largest banks.

"Security at a data center is a marriage between the physical asset and the process side," Holmes explains. "We focus a lot on the threats that are particular to this business. For example, in the Washington D.C. area, there's always the potential for protestors, so we have to be attuned to whether our tenants are liable to be attacked. We work on a list, from the highly unlikely to the very possible, and then present the case to senior management."

Holmes uses a variety of security practices to secure the data center, which he says includes an eight-foot high perimeter fence, heavy grade interior windows, no exterior windows, a 24-hour guard service from Securitas, palm and fingerprint readers and biometric eye scanners.

The same can be said at Retirement Systems of Alabama (RSA), which manages public pension funds for state and local employees and public education employees in the state of Alabama, and operates the Dexter Avenue Data Center in Montgomery, Ala.

John Hill, CTO, explains: "First, complete background checks are done on each visitor, and video entry is everywhere. Next, from the minute someone walks in the door, they are under complete observation; there are no gaps. They need complete credentials to even access a floor in the elevator. To get to the data center floor of the Dexter Avenue building, you first enter a turnstile with a biometric credential. Once you step out of the elevator, there are additional biometric readers to get you to the next step. That type of security takes place every step of the way."

Hill worked with Larry Oliver with systems integrator Vision Security Technologies, which is a Security-Net member company. Hill notes that specific security in place at RSA includes an underground high-reliability network power feed from Alabama Power with three transformers, emergency generators, 4,000 gallons of on-site diesel fuel, APC racks with HID readers front and back, a Clean Agent Fire Protection System and more. SECURITY

Want to Learn More About Securing a Data Center?

Attend the Anixter Data Center Seminar Series, Data Center Physical Security, on August 16, 10:30 am CST. Register today at SecurityMagazine.com/DataSeminarSeries