

Security from the First Step

In survey after survey done by IDG Research Services, security remains a top concern for CIOs. For example:

- 63percent of IT executives invested in data security tools in 2007
- 93percent of IT executives cite security among the top five most important factors when evaluating and selecting IT products and services, ahead of total cost of ownership.
- Security ranks among the top five most appealing aspects of Storage-as-a-Service.

Knowing that data security is a top concern for its customers, Iron Mountain Digital recommends, and itself builds in security features from the very beginning of the product development process. “We’ve got all these products that we ship that really need to protect our customers,” says French. “Security isn’t bolted on to the application; it needs to be part of the design process.”

Best practices mandate that a corporate security team sets the requirements for the products. Once the application code has been written, it undergoes rigorous security reviews to make sure there are no vulnerabilities. Then the products enter a quality-assurance phase, internal penetration testing and external third-party validation. “Security is in the beginning, we’re doing code analysis in the middle, we’re doing security testing in-house, and we’re doing third-party independent validation,” says French. “We bake it into the process.”

Safeguarding Customers’ Data

Beyond building security into its products from the initial development stages, best practices dictate that customers’ data is kept secure all the way through the backup and storage process.

No more open ports

In a typical client/server backup model, a server periodically sends a request to a client in a PC or a remote server and collects changes that have occurred since the last backup on the client side. The danger here is that this model leaves ports open, which can invite attacks from hackers. Iron Mountain takes the opposite approach. For example, Iron Mountain’s Connected installs a small agent on the PC that always initiates the conversation with the data center, leaving no ports open and unprotected. Only eligible agents have access to the data center. “We don’t allow the open ports to be there,” says Su.

Encryption

Encryption plays a considerable role in protecting any data transmitted for offsite storage. As a required com-



“You’re only as secure as your weakest link,” says Jackie Su.

ponent, when companies choose Storage-as-a-Service, they gain access to the provider’s encryption knowledge, expertise and flexibility. For example, customer data is always encrypted before passed through a secure transport to the provider, which stores it on their side.

With some data storage models, an encryption key is stored along with encrypted data, leaving open the door to a hacker who could potentially obtain both the data and the key to restore the data. However, in the most secure model, Su explains, only the agent holds the key to restore the file; it stays separate from the encrypted data. At the same time, mutual authentication should be used to unlock the data when necessary. The authentication involves a random algorithm adding another layer of security should any unauthorized person attempt to gain access to the key.

This focus on encryption protects customers from both external and internal threats—an appealing aspect particularly in industries that deal constantly with sensitive data. If companies entrust sensitive financial or medical data, for example, to a third-party storage provider, they need to be certain that the provider’s employees can’t access that data any more easily than a hacker can.

Physical security/disaster recovery

When it comes to backing up and recovering stored

data, a secure underground data center is paramount for data protection. As an example, Iron Mountain's underground vaults feature 24/7 armed security, a Tier 3 security rating, a Bruns-Pak rating of 9 (Brunns-Pak Corp. of New Jersey rates data centers on a 1-10 scale, with 10 being a "State of the Art" data center; a "9" rating is "Ultra-Reliable Data Center."), an OSHA-certified company, and other features that ensure the safety and security of data. (For the sake of comparison, the Pentagon is Tier 4.)

"This is our bread and butter," says French. "Not many companies have a data center 220 feet underground that could survive natural disaster."

A Complicated Regulatory Landscape

In the days before heavy regulations in the insurance, health care and banking industries, storage providers found themselves dealing mostly with the IT department.

"Now, with the compliance and regulation problems becoming more predominant, the security folks, including the CSO, are very concerned about how the [storage] company's policies and processes will mitigate risk," says Su. Storage decisions today often involve corporate counsel and executive-level decision makers. With regulations like Sarbanes-Oxley, FRCP Rule 26 and HIPAA as well as from the Securities and Exchange Commission forcing companies to rethink their infrastructure and privacy mechanisms, storage and backup become not just a luxury but a necessity.

"A lot of the best practices that we have built into the technology we've done because of how they will help customers in a compliance situation," says Su.

Even industries like retail—in which a few very highly publicized breaches have recently called into question the way companies safeguard their customer data—have become very proactive about how secure their data storage is.

"I think everyone has realized that if you're a big company, you're going to be a target, and you have to do your due diligence irrespective of what vertical you're in," French says.

The Future of Storage and Security

If there's one thing that's certain about the future of data storage and security, it's that the picture isn't going to get any less complicated. Some of the changes businesses of all stripes can expect moving forward:

Data lost equals big money lost

According to a survey conducted by Ponemon Institute in 2007, the average cost of a data breach is \$6.3 million. That means data storage concerns will continue to migrate

pretty rapidly from the back room to the boardroom, no matter what vertical market a company serves. "A data breach has a huge brand and revenue negative impact no matter what industry you're in," says Su.

Globalization and scattered standards

"Things are scattered, and I see that getting worse," says French. With different organizations and countries setting different standards for encryption, certification and best practices, companies will need to spend more manpower keeping up with changes. "There's going to be a lot of confusion about what's good and what's bad from a compliance and certification perspective," he adds.

Mobile devices will change the landscape

The more businesses integrate mobile devices like the BlackBerry and the iPhone into their work practices and their culture, the more confidential data will become vulnerable to loss or attack, and companies will find it increasingly difficult to balance the novelty of new technology with the risks.

"Companies assume a great deal of risk when they take a do-it-yourself approach in areas that are not their core competency, especially when it comes to information protection and management."

Social networking

As more knowledge workers employ social networking tools, and as the lines between the personal and the business worlds continue to blur, corporate security concerns will become both broader and more difficult to address. "You can't stop people from exchanging information," says Su. "The risk is always there."

For all these reasons, businesses will turn more and more to trusted partners whose expertise lies in storing and security data. "Human behaviors always repeat themselves. To eliminate human error is a very, very difficult task," says Su. "The best thing to do is to have a lot of checks and balances in place. It's important to choose a vendor with proven know-how, processes and technology to reduce the costs and risks associated with your data protection needs." ▲

MEG MOORE IS A FREELANCE TECHNOLOGY WRITER BASED IN MASSACHUSETTS.