

## The Security Arms Race

### CSO's job is not getting any easier

By Aaron Bills

Why is enterprise-level information security so difficult to manage? This question always seems to surface whenever a major credit card data breach occurs, like those announced recently by the Hannaford supermarket chain and the Okemo ski resort in Vermont.

Managing information security in large organizations is a dynamic, complex task with multiple operating components, resource needs and requirements that constantly change. Managing and optimizing technology operations and resources so they're well-protected requires, among other things, configuring data centers and firewalls against possible intrusions, updating core systems and assets such as hardware, software and network architecture as well as staying abreast of IT governance requirements.

Think of an enterprise as a sphere. The bigger it gets, the more surface areas there are to cover. And as an organization grows, the radius of the sphere expands along with its vulnerabilities and administrative requirements - all of which make the CIO/CISO's job more challenging.

Security is also contextual, depending on the environment in which the organization operates and the circumstances that expose its vulnerabilities.

As a business grows, responsibility for protecting customer cardholder data also grows exponentially in terms of risk and compliance requirements.

Last fall Forrester Research reported in its State of PCI Compliance study that more than 100 million personally identifiable customer records had been breached in the U.S. over the past two years and that most of these breaches occurred at companies with household names. Forrester asked 677 IT security executives from the U.S. and Europe about their data retention practices and found that 81% store credit card numbers, 73% retain card expiration dates and 71% keep verification codes on file.

With this amount of sensitive payment data being retained, it's vital that proper controls be in place. Even if merchants use state-of-the-art technologies to store the data internally, they need to minimize, to the greatest extent possible, the points at which credit card data is handled because the risks and impacts from a security breach could be devastating. While the direct consequences of a company suffering a breach often involve substantial fines and other expenses, the most long-lasting effects are typically customer turnover, brand erosion and loss of corporate reputation.

The payment industry has taken exceptional strides to self-regulate and promote data security, including establishing rules known as the Payment Card Industry (PCI) Data Security Standards. While becoming PCI-certified does not magically shield a business from losing data, it does mean that they have protective policies and controls in place to support secure handling of confidential credit card information.

But despite all the sophisticated security technologies on the market today, merchants of every size and shape continue to face growing risks when processing sensitive card data, and ensuring proper safeguards are in place is especially difficult when they store card data themselves.

One of the safest practices for merchants who process credit card data is so obvious it is often overlooked: eliminating the storage of that data altogether.

*Aaron Bills is the chief operating officer and co-founder of 3Delta Systems.*