BIG DATA: DREAM OR POTENTIAL NIGHTMARE?

BY MARK GERENCSER

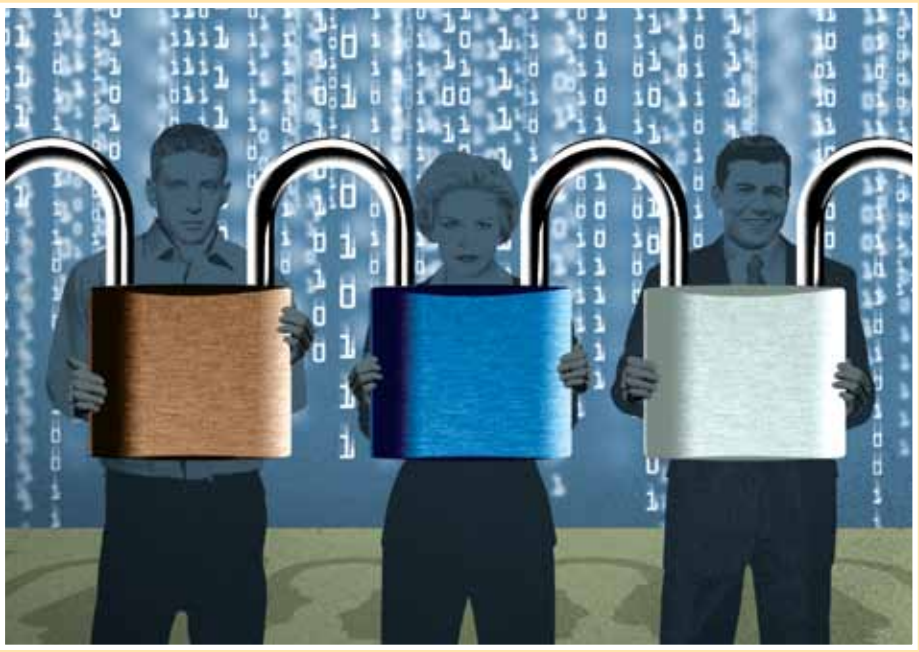

ILLUSTRATION BY JOHN RITTER

THE AMOUNT OF INFORMATION about us—the products we purchase, the processes we use, and the businesses that surround us—has grown exponentially. We now generate more data every two days than we did in aggregate from the dawn of early civilization through the beginning of the 21st century. And this information explosion accelerates each year by 40 percent. This is called the "Big Data Revolution" and it is not only big in volume; it is also big in variety and velocity—meaning different types of data at a wide range of input speeds and refresh frequencies. Big Data has very *big* implications for business.

Big Data offers a company numerous opportunities to enhance its value across entire product and service lines based on advanced analytics. For example, an airline might dynamically optimize fares based on customer preferences and behavior, or an electric utility might optimize power generation and distribution based on consumer needs and living habits.

Some challenging questions revolve around data rights and ownership, and it will take some time for a consistent legal framework to emerge. In the interim, though, Big Data's business advantages are offset by each company's responsibility to protect private, personal, and sensitive corporate information.

Leaders must know the answer to several key questions: Where does your company stand amongst your peers with respect to data security? Are you leading with best practices or lagging behind? Do you understand and appreciate your liability? Do you have a plan to address deficiencies?

Because the cyber threat environment is rapidly advancing, traditional security methods are not just incredibly expensive; they no longer work. "Attack surfaces"—the ways a company's data can be exploited—are increasing, even as attack methods are becoming more sophisticated. Responsible corporate leaders must understand their attack surfaces and the effectiveness of their security measures. We have found many companies don't get the most for their security expenditures, and some spend more than their peers but get less in return. Since there are no absolutes in security, peer benchmarks provide the best measures of effectiveness.

Companies need to think and act differently to get the most for their data security investment. This includes collaborating with others in their industry, even competitors. Every enterprise needs to understand the risks they assume and what they mitigate relative to one another. Companies that lead in this area will be advantaged as trusted partners and providers, which in turn will benefit sales and customer retention. It also promises to reduce liability in the event of data spills, insider disclosures, or remote data theft or destruction.

Through collaboration, companies can create reasonable standards that may serve to head off more restrictive governmental regulations. But peer collaboration can provide more than just reasonable standards for an industry; it might also identify opportunities to share security investments and approaches. For example, the electric utility sector could develop a cooperative to monitor and identify imminent attacks on the power grid, spending less on static security and instead focusing resources when and where they are needed.

While IWCA (indication and warning and counterattack) capability has proven effective, it is seldom affordable for an individual company; however, a shared cost approach could provide high value at significant savings. Our experience shows that once an IWCA capability has been established, adding companies in the

continued

PHOTOGRAPH BY DANUTA OTFINOWSKI

Mark Gerencser is chair of UMUC's Board of Visitors and co-author of the best-selling book, *Megacommunities.* He is managing partner of Booz Allen Hamilton's Global Commercial Business, the leader in enhancing company operating performance, regulatory compliance, and security.

BIG DATA: DREAM OR POTENTIAL NIGHTMARE?

continued

same industry category increases value at only a slight increase in operating cost. This makes a community or shared services approach practical, affordable, and effective.

In short, Big Data presents corporate leadership with new business opportunities—and new responsibilities. The opportunities vary greatly by industry, but the responsibilities are fundamentally the same: the protection of personal, corporate, and sensitive data. Data security strategies must shift from the expensive static approaches of the past to the more cost effective, dynamic, and collaborative approaches of the future. The market will ultimately reward those companies that capitalize on opportunities and take the necessary steps to ensure data security. ✧