RFCODE

White Paper

Big Data. Bigger Security Risks:
How Data Centers Can Track, Manage, and Secure Data with Dedicated Asset Tracking Networks

Executive Overview

Companies are spending billions of dollars to fight the threat of cybercrime by deploying processes to keep hackers out of their systems and away from their data. Meanwhile, many of today's most damaging security breaches occur, not from outside companies, but from within.

Many of these internal data breaches are the result of simple negligence, including misplaced, lost, and stolen devices on which the data is stored. This internal security threat is every bit as serious, if not as sensational, as external threats — and comes with the same high cost regulatory penalties, lawsuits, and PR nightmares. Plus, every incident adds an additional element to the equation — embarrassment. After all, in today's world of sophisticated technology, the public wonders: How can a company misplace a critical device containing customers' private data?

Making matters more urgent is the fact that the data that companies are acquiring is getting bigger. This big data comes with even bigger security risks. In the face of bigger and bigger stores of data, and an ever-tightening regulatory system, it's time for companies to implement systems that centrally track every device in their data centers — from the time they are purchased all of the way to their end-of-life disposal. This white paper highlights the factors driving big data growth and the increasing demand for greater control and tighter data security, not just from threats outside of the data center, but from negligence inside companies, as well. The white paper offers a solution that gives data centers 100 percent tracking control over every device across their entire network.

State of the Industry — The Big Data Driver

The term "big data" has been used extensively over the past few years. But what is it? It refers to the petabytes of data that are being gathered everywhere in the digital age at a furious pace and by multiple devices, including mobile devices, cameras, microphones, passive RFID readers, and wireless sensor networks. Already most large corporations are sitting on mines of data simply by virtue of their vast networks and everyday operations. In 2011, IDC estimated that 1.8 billion terabytes of data were created, 90 percent of which was created in a non-structured fashion. IDC further projects that unstructured data will grow at more than 60 percent compounded annually.

What will companies do with all of this data? Experts say that big data presents an opportunity to perform increasingly sophisticated analysis faster and with clearer insight. This business intelligence will create unprecedented business advantages, including understanding customer product preferences, spotting user pattern changes, assessing service delivery specifications, and creating competitive advantages. Research conducted by the McKinsey Global Institute points to big data having the ability to generate significant value and commercial impact, such as a 60 percent potential increase in retailers' operating margins, and 0.7 percent increase in productivity in U.S. healthcare, which translates into a value of $300 billion per year.

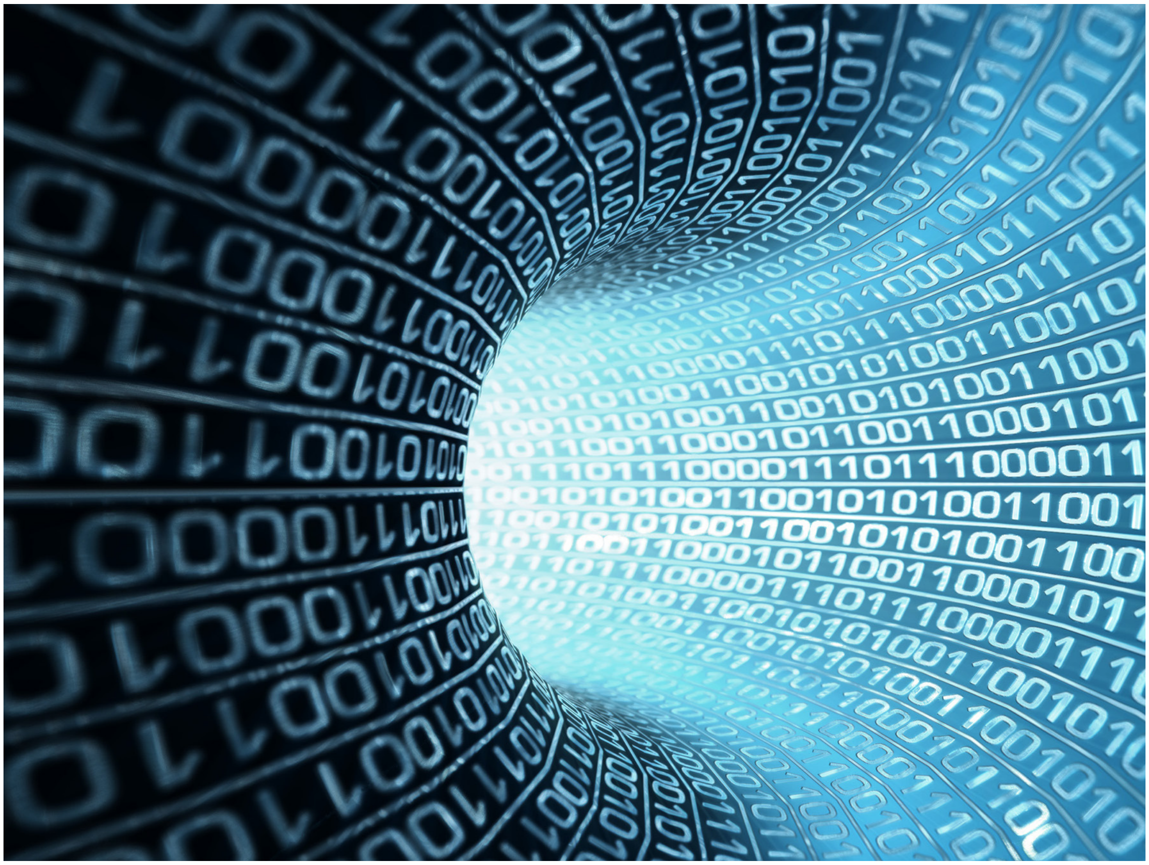
According to a worldwide survey of IT leaders conducted by Gartner in 2012, 42 percent of respondents said they had invested in big data technology or were planning to within a year. "Organization have increased their understanding of what big data is and how it could transform the business in novel ways," said Doug Laney, research vice president at Gartner. "Big data has become critical because it has obvious or potential business opportunities that cannot be met with traditional data sources, technologies, or practices." But "most organization are still in the early stages, and few have thought through an enterprise approach or realized the profound impact that big data will have on their infrastructure, organizations, and industries" — including internal data security.

As big data becomes a potential game-changer for businesses, and larger amounts of data are generated, analyzed, and stored, the security risks and privacy issues become even greater. Today's levels of legislative and regulatory requirements are bound to expand right alongside big data's growth. This includes jurisdictions outside of the U.S, wherever data is stored and customers are based, because companies holding foreign data will fall under foreign as well as local jurisdictions and regulations.

Despite these challenges, by 2015 Gartner predicts that 20 percent of Global 1,000 organizations will have established a strategic focus on big data information infrastructure equal to that of application management. The research firm says that companies in a wide variety of industries are provisionally collecting and storing a burgeoning amount of operation, public, commercial, and social data in anticipation of being able to make use of big data technologies. In the meantime, all of that data needs to be kept secure.

Internally Created Data Security Incidents on the Rise

Data hacking scandals grab all the headlines. But there are other monster security risks that are just as damaging — and they don't come from outside the company. They come from internal mistakes and negligence, like losing the devices on which data resides. Every year there are hundreds of cases of missing data, due to misplaced, lost, and stolen devices in healthcare, banking, insurance, government, and other industries. Here are just a few of the hundreds, even thousands, data security disasters that occur from within companies' networks.



- **Lost in Transportation.** In April 2012, Canada's Toronto-Dominion Bank, disclosed a security problem of its own making — the loss of 260,000 customers' data, including Social Security numbers and bank account information, on two server back-up tapes that went missing while being transported from one location to another. The incident cost the bank significantly in terms of public relations, lost customers, regulatory fines, and future scrutiny.

- **Missing in Inaction.** In February 2012, Emory Healthcare lost ten computer disks containing encrypted personal information on over 300,000 patients, including patient names, diagnosis, surgical procedures, surgeons, and Social Security numbers. The disks went missing from an office where they were being stored. As a result of the major data breach, Emory Healthcare faced HIPAA fines, a HIPAA breach violation, and a class action lawsuit for $200 million dollars.

- **Moving Violation.** In 2011, the Department of Defense was hit by a $4.9 billion class action lawsuit filed on behalf of four military family members and 4.9 million Tricare beneficiaries whose personal information, including Social Security numbers and clinical notes, was contained on back up tapes stolen from an automobile.

- **Recklessly Abandon.** In 2009, Blue Cross Blue Shield of Tennessee paid $1.5 million settlement after losing 57 hard drives containing data on more than one million customers due to a burglary. Blue Cross was fined $1.5 million by the U.S. Department of Health and Human Services. But the fine was less than 10 percent of the true cost to Blue Cross, which so far has spent $17 million in corrective actions.

Why the Problem of Securing Data Will Get Worse

As companies collect more data across their enterprise, security concerns will escalate exponentially. Further, corporations will be forced to look increasingly at outsourcing their stores of data as their own data centers reach capacity. But this move won't hold them harmless from negligence when data is lost, stolen, or misplaced. As the regulatory reigns tighten around data security and privacy, CFOs will increasingly be under fire for any security breaches. Already CFOs are taking the hit for mistakes made, whether they were directly responsible or not.

Big Data is Growing Bigger

An article in Information Week in August 2012 highlights the numerous concerns that come with handling big data, including securing big data. These security issues are nothing new, but the need to address them has never been more pressing as they become magnified by the sheer volume, variety, and velocity of big data. The most frequently discussed problem is that of data theft from outside the company. But this isn't the only worry. Other problems include cloud storage, employee access, the vulnerability of interconnected supply chains that rely on data, and privacy concerns. All of these issues have the potential to create a disaster for companies that don't get their systems under their control.

Storing and analyzing big data can be rife with security risks, according to a Forrester Research report issued in May 2012 entitled The Future of Data Security and Privacy: Controlling Big Data. "It is imperative that users of the data understand that these massive data stores contain significant amounts of 'toxic' data," says Forrester analyst John Kindervag. "Toxic data is any data that could be damaging to an organization if it leaves that organization's control. Typically, toxic data includes custodial data — such as credit card numbers, personally identifiable information like Social Security numbers, and personal health information — and sensitive intellectual property, including business plans and product designs."

Data Storage Hitting a Wall

In the face of exploding quantities of data, in the U.S. alone data storage requirements are driving up floor space needs. Some predictions say that companies will run out of data center floor space by 2015. Even virtualization technologies and "the cloud" aren't reducing the floor space requirements, because the data still has to reside somewhere — and that is on devices housed in data centers.

In 2012, in the U.S. there were nearly three million data centers, server rooms, and data closets, according to the IDC. These data centers had a total capacity of 611.4 million square feet of floor space: The aggregate floor space in those data centers is expected to rise to 700 million square feet. In the face of impending data center limitations, many companies are turning to co-location facilities. IDC is projecting that by 2016, more than a quarter of the data center floor space in the U.S. will be owned by service providers. However, storing data outside of a company's walls does not relieve companies of their responsibility for the data's security.

CFOs in the Crosshairs

As data expands, the importance of information security is becoming a pressing concern in corporations, and nowhere is that more clear than in the CFO's office. Data protection used to be the responsibility of IT personnel and the Chief Information Security Officer (CISO). But the surge of data breaches has forced finance departments to increasingly collaborate with IT departments on developing security policies and dealing with data loss incidents. According to CFO magazine, many CFOs are facing a "rude awakening": the scope of their liability is growing markedly, to the point where unforeseen liability lurks seemingly around every corner. For example, under the Dodd-Frank Act, which gives the Securities and Exchange Commission (SEC) broad enforcement powers and also heightens the standards for management of internal controls, the SEC can now bring a claim for aiding and abetting a violation of any of the federal securities statutes without having to establish that the accused party acted with "actual knowledge." Now, recklessness is sufficient to establish a claim of aiding and abetting.

CFOs and other executives face growing numbers of enforcement and civil actions arising from these provisions. In fact, there has been a growing number of prosecutions in which CFOs face penalties, whether or not they knew that the activity was unlawful, if they simply failed to supervise subordinates adequately, or if they certified corporate financial statements that later had to be revised due to another employee's wrongful conduct. As a result, data security is the number one issue in the boardroom, according to an annual survey of general counsel and corporate directors of public companies by FTI Consulting and Corporate Board Member.

An Action Plan for Dedicated Asset Tracking Networks

The most powerful and cost-effective way to gain control of data internally and reduce the risk of internal security mistakes is to track every physical asset continuously and in real-time for the entire life cycle of the device. One technology provides this comprehensive level of device micro-management — dedicated asset tracking networks.

Dedicated asset tracking networks provide companies with a powerful and convenient way to centrally track every single device across their networks, no matter how remote — from the moment a new device enters the system until it reaches end-of-use disposal. Asset tracking networks consist of three main components: asset tags, readers, and software.

- **Device Tracking Asset Tags.** Active RFID tags are affixed to each asset. The tags automatically beacon tag identifier numbers at regular intervals, such as every 10 seconds. This provides a constant stream of device information without requiring any human interaction.

- **Device Tracking Readers.** Readers are strategically placed within the network. They receive the beacons that the asset tags transmit.

- **Device Tracking Software.** The software receives the data from the readers and transmits the location of every asset within the facility. Tracking can be configured at a room level, rack level, or zone level, where the software reports which reader a device is closest to. IT staff can centrally manage asset tracking across the entire network.

Conclusion

IT organizations are under increasing pressure to deliver more functionality — faster and with tighter budgets — to service their businesses and their customers. This pressure will only increase as companies expand into the world of big data. Companies will face massive implications for losing track of their data, including steep regulatory fines, greater regulatory scrutiny, class action lawsuits, PR nightmares, lost customers, and investor wrath. These internal data security challenges cannot be mitigated with existing systems like firewalls and back ups. They can only be contained by deploying intelligent technologies designed specifically to track physical assets and the data that sits on them. Anything less than 100% device micro-managed tracking is no longer enough. There are way too many opportunities for exposure — and too many negative consequences from internal negligence.

The pendulum has swung toward dedicated asset tracking solutions that continuously micro-manage physical assets across the network. Early-adopters of dedicated asset management networks are already gaining complete control over their devices, and are enjoying peace of mind in knowing their assets that store data will not be lost, misplaced, or forgotten. They know where every server, storage device, computer, and other sensitive equipment is located in their network at all times — and, as a result, they know exactly where the data that lives on those devices is as well. Dedicated asset tracking networks are the safest way to close the holes of internal security breaches — and rest assured that data is not languishing in a closet, transported in an unsecured fashion, or otherwise lost due to internal human error.

About RF Code

RF Code provides end-to-end data center asset management, environmental and power monitoring solutions. Its unique combination of powerful software, intelligent infrastructure and internet-connected, wire-free sensors reduces operational costs and protects your data center investments. RF Code solutions deliver continuous location visibility throughout an asset's entire lifecycle while accurately monitoring temperature, humidity and other environmental factors that can damage assets or lead to costly downtime.

Featuring the sophisticated reporting, alerting and analytics that data center operators demand, RF Code's fully automated solutions enable real-time, data-driven capacity planning and management policies that increase efficiency, eliminate manual processes, ensure regulatory compliance and deliver an immediate return on investment. Founded in 1997 and headquartered in Austin, Texas, RF Code has offices and partners in the UK, EMEA, Australia, Asia and South America.

RFCODE
9229 Waterford Centre Blvd. ♦ Suite 500
Austin, TX 78758
Tel: 512.439.2200 ♦ Fax: 512.439.2199
sales@rfcode.com ♦ http://www.rfcode.com