2015 Manufacturing &
Distribution Monitor Report

Information technology and data security

McGladrey

Assurance ▪ Tax ▪ Consulting

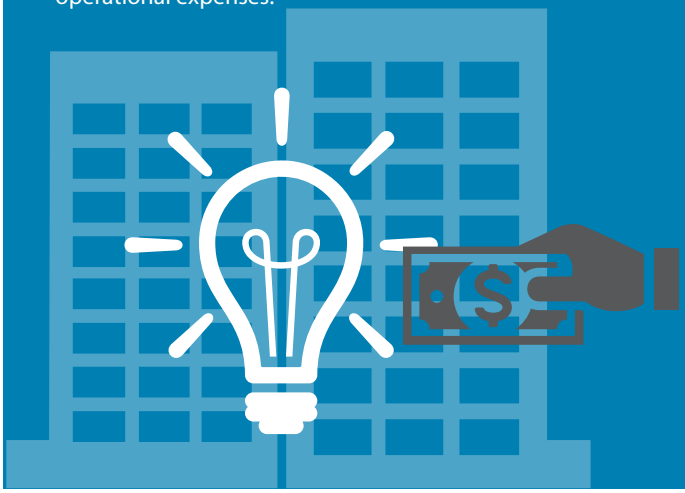
OVERVIEW OF FINDINGS

NON-U.S COMPANIES

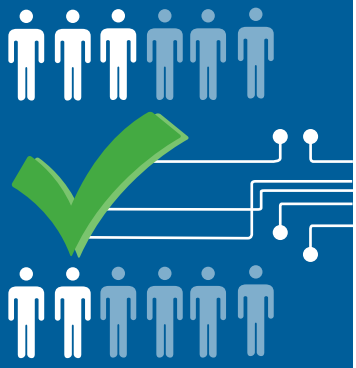
lead U.S. companies in the successful implementation of **12** major areas of technology.

KEEPING THE LIGHTS ON

U.S. companies are investing in IT, but these dollars are being spent primarily on operational expenses.



Emerging technologies have been successfully leveraged in **HALF** of non-U.S. companies compared to **ONE-THIRD** of U.S. companies.

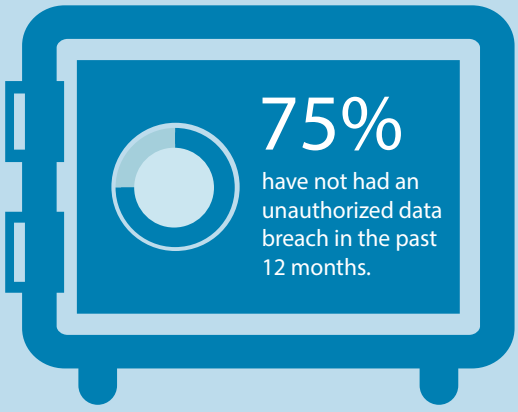


INVESTMENT TRIGGERS

52% SAY CUSTOMER REQUESTS AND CLIENT-FACING FEATURES are the primary triggers for technology investments.

#2 trigger for U.S. manufacturers is **SYSTEM FAILURE**

EXPERIENCE WITH A DATA BREACH?



75% have not had an unauthorized data breach in the past 12 months.

11% don't know if they have had one or not.

MONITOR AND SAFEGUARD

63% SOMEWHAT OR NOT AT ALL CONFIDENT in their current ability to monitor and safeguard sensitive customer data from unauthorized access.

TWICE as many non-U.S. companies expect their investments in cybersecurity will drive growth in the next 12 months.

U.S. companies overall only invest **6%** of total IT spending on security and risk management.

Technology as a competitive advantage

A common perception of U.S.-based businesses is that they are the *avant-garde* of information technology. The country is, after all, home to the 10 largest tech companies in the world, as measured by market capitalization.[1] So it is understandable that the collective efforts of U.S.-based manufacturers to leverage emerging technologies are assumed to be the very definition of cutting edge. The competitive advantage these businesses gain from their use of the latest in data analytics, operational efficiency and information security should be the envy of the rest of the business world. The reality, however, tells a slightly different story—one that the U.S.-based companies need to understand.

Overall, U.S.-based companies are lagging behind non-U.S. companies in their use of information technology (IT). According to the 2015 McGladrey Manufacturing & Distribution Monitor, non-U.S. companies participating in the survey are leading in successful implementation in almost every IT category, from cloud computing and mobile technologies to customer relationship management and emerging technologies to big data analytics and social media. There is a higher percentage of non-U.S. companies (72 percent) planning to increase their IT investments in the next 12 months than U.S. companies (66 percent); a greater percentage of non-U.S. companies than U.S. companies see the possibility of planned investments in cybersecurity driving growth (29 percent and 15 percent, respectively).

This report is part of a series taking an in-depth look at how manufacturers and distributors are investing their time, efforts and resources in global growth, innovation and information technology. In particular, this report examines notable IT-related highlights from the 2015 Monitor.

There were 1,660 respondents to the 2015 Monitor survey, which was conducted in March and April 2015. Participants were primarily C-level executives from chair to chief information officer, most of whom (65 percent) were at companies based in the United States; the remainders were from companies based throughout Asia, Europe, Brazil, Canada and Mexico.

The insights provided by these executives regarding information technology illustrate the critical need for U.S.-based companies—particularly those in the middle market—to be proactive in their strategic use of technology—in order to manage supply chains, run operations, mitigate risks effectively and, ultimately, compete in an increasingly global market place.

A technology wake-up call

During the economic downturn, technology-based initiatives often did not have budget allocated to keep them up to date. Without consistent upgrades and IT investment, the legacy systems at many companies quickly became outdated (this is sometimes known as a company's "tech debt").

Yet despite the growing strength of the current economy, U.S. companies, by and large, dedicate only about 3.3 percent of revenue to technology.[2] Even in an era of high-profile and costly information breaches, companies overall only invest roughly 6 percent of total IT spending on security and risk management. These companies lose advantages they may otherwise have over competitors who implemented upgrades as new technologies became available.

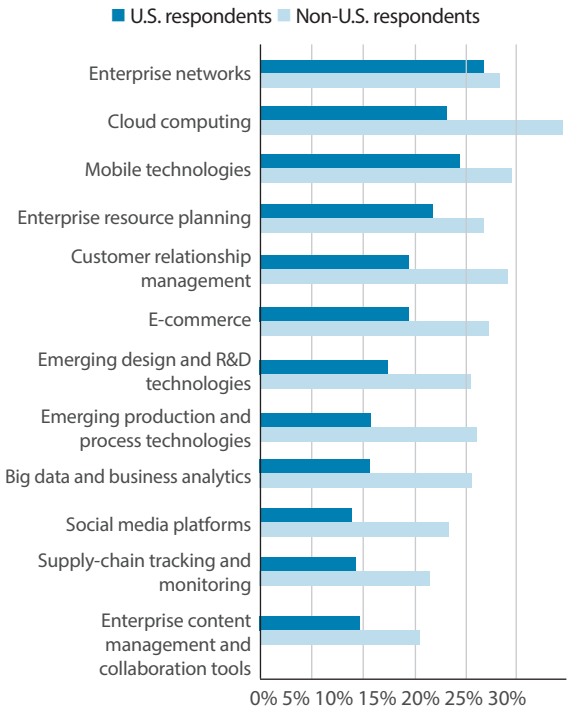
The investments made by non-U.S. companies show more diversity and are achieving a greater percentage of successful implementation than investments made by U.S. companies.

Leveraging technology to drive success

From enhancing customer service with personalized solutions to increasing efficiencies in production and distribution, manufacturers are making strategic use of technology in a range of services as well as management and production tools. Yet the investments made by non-U.S. companies show more diversity and are achieving a greater percentage of successful implementation than investments made by U.S. companies (Figure 1):

While a majority of businesses participating in the Monitor utilize ERP technologies, ECM and other collaboration tools are more prevalent outside of the United States, where 41 percent of non-U.S. manufacturers are leveraging these technologies, as compared to only 27 percent of U.S. companies.

FIGURE 1. Successfully implemented IT systems



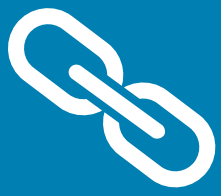
According to a report by The Conference Board, the use of big data analytics technologies—a top issue in 2014 for chief executive officers in general around the world—is less of a concern this year. The report suggests that this indicates that CEOs may be trying to implement and utilize these technologies.[4] But for manufacturers, however, usage may vary by region. The percentage of non-U.S. Monitor participants who have had some or significant success in implementing big data and business analytics tools (45 percent) exceeds that of U.S. companies (33 percent)—with just under half of U.S. companies (44 percent) saying they have no plans to take advantage of all that big data tools have to offer.

LEVERAGING TECHNOLOGY TO DRIVE SUCCESS

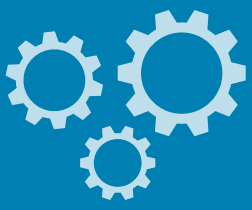
E-COMMERCE According to the U.S. Department of Commerce, e-commerce sales accounted for 6.5 percent of total 2014 sales, which represents a 15.4 percent increase over 2013.[3] For non-U.S. companies, e-commerce is an important and relatively low-cost method for breaking into the attractive U.S. market. This may account for the significant success, according to the Monitor, among these companies in implementing e-commerce technology (22 percent) compared to U.S. companies (14 percent).

CLOUD COMPUTING The cloud replaces some or all of a company's hardware, facilities and software licensing with an outsourced provider, reducing management's burden to house and maintain them on-premises. Due to a lack of understanding of benefits and apprehension regarding IT data security, among other concerns, U.S. companies may still be somewhat reluctant to transition to the cloud; only 18 percent of U.S.-based Monitor participants have experienced significant success with the technologies, compared to 29 percent of non-U.S. participants.

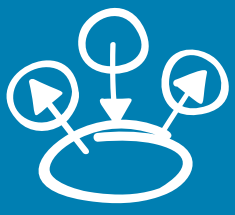
MOBILITY SOLUTIONS A changing, more-connected workforce is driving mobility adoption, as real-time information is expected and is more readily available than ever. Mobility is having an impact on many organizations' supply-chain strategies, for example, providing increased data access from any location and capturing targeted information at the source. As identified in the Monitor, both U.S. and non-U.S. manufacturers (59 percent and 62 percent, respectively) have experienced some level of success in implementing and leveraging mobile technologies.



SUPPLY-CHAIN TRACKING AND MONITORING The key to effective supply chain management is to use real information that reflects actual demand in the supply chain rather than rely on forecasts. Technologies such as radio frequency identification systems present a major opportunity for manufacturers and distributors to increase efficiency and visibility into operations while decreasing costs. According to the Monitor, these transformative platforms are being successfully leveraged by a much greater percentage of non-U.S. companies (45 percent) than U.S. companies (31 percent); in fact, 45 percent of U.S. manufacturers have no plans to implement them.



PRODUCTION AND PROCESS Many of the opportunities companies are identifying and the products and services they are offering have come about as the result of the phase in technological development first discussed in 2008 and popularly known as the third platform, an aggregation of several technologies, including mobile components, cloud computing, social media, big data and the Internet of Things. As seen in the Monitor survey, emerging process technologies are more prevalent outside of the United States.



MANAGEMENT AND PLANNING Enterprise content management (ECM) applications can help track unstructured data, that is, all of the documents, forms and processes that encompass all roles—storing and managing documents as well as facilitating workflow. Customer relationship management (CRM) solutions are evolving, with new strategies to further integrate critical business processes. Big data is designed to take information from disparate sources and provide insights not normally available through traditional means. Enterprise resource planning (ERP) systems can standardize forecasting processes and eliminate data entry duplication. The right systems capabilities can leverage best practices to save time and money.

What is driving technology investments?

For just over half of non-U.S. Monitor participants, customer requests and client-facing features are the primary factors that trigger technology investments. The innovative products or practices of a competitor as well as regulatory changes are the next most-cited drivers.

In the United Kingdom, nearly two-thirds of Monitor participants have consumers and retailers as core customers; this is driving investments exceeding those by U.S. companies in a range of consumer-oriented technologies, including CRM, e-commerce, social media platforms and mobile technologies.

For just over half of non-U.S. Monitor participants, **customer requests and client-facing features** are the primary factors that trigger technology investments.

Across the European Union, the successful implementation of these technologies is even more extensive as EU companies seek to break into markets outside of their borders. Because their domestic markets are relatively small, EU manufacturers tend to export or internationalize their businesses earlier than their U.S. counterparts. This pushes them to invest in ERP systems earlier as well in order to manage the complexities of international reporting and regulatory requirements. Deregulation of European markets has promoted cross-border trade significantly over the past two decades, further providing incentives for expansion and, as a result, IT investment.

In Brazil, where high workforce costs are intransigent and the demands of the Brazilian revenue services are extensive, technology is one of the only ways to cut operational costs and ensure compliance in a complex regulatory environment. "Given the intricate nature of their country's tax codes and regulatory obligations, Brazilian companies are successfully implementing relatively simple, low-cost and flexible software suites," says Wesley Montechiari Figueira, a senior partner at RSM Brasil.

Countries with emerging economies struggle with establishing a culture of investment. As such, companies in countries like Mexico invest in ERP systems as they are generally easier to implement than CRM technologies. As business conditions improve, an increasing percentage of Mexican companies participating in the Monitor found success in implementing both technologies.

Around the world, there also are sanctions for data breaches and privacy issues that provide incentives for implementing data security policies and procedures—and some penalties can be quite serious. Regulations such as the Consumer Protection and Defense Code in Brazil or the Privacy and Electronic Communications Regulations in the United Kingdom, for example, can penalize individuals as well as corporations for violations of privacy. Fines imposed on corporate entities can be as high as €1.5 million ($1.6 million) (France); and/or imprisonment from six months (Argentina) to five years (Taiwan). In Brazil, there are no legal provisions or standards specifically established for data privacy violations by Brazilian companies, so penalties are determined by the court.[5]

Business conditions certainly are a factor as companies prioritize their IT investment choices. For example, concerns about customers, competition and data security drive IT investments for a greater percentage of thriving companies than for declining companies; this holds true for both U.S- or non-U.S.-based companies.

What is striking is how regulatory changes are prioritized. The percentage of non-U.S. companies making IT investments due to regulatory changes is relatively flat, regardless of the business condition, at about 33 percent. For U.S. companies, however, there are significant differences. As U.S. companies thrive, regulatory issues provide a greater impetus for IT investment: 34 percent of thriving companies as compared to only 18 percent of declining companies invested in IT for this reason. For these thriving U.S. companies, the complexities that come with growth may be driving more companies to give a higher priority to their IT investments.

Where are companies investing?

To be clear, this is not to say that U.S. companies are not making strategic investments in their IT environments—they are budgeting for technology, but not to the degree of their overseas competitors. And make no mistake: Those overseas companies are continuing to become greater competitive threats to those in U.S. markets.

In Europe, the comparative maturity and low cost of offerings such as cloud and mobile technologies, along with the increasing availability of high-speed broadband, may help explain the significantly higher percentage of Monitor participants that have successfully implemented emerging production and process, cloud computing, CRM, supply chain tracking and other technologies. Cross-border trade has been encouraged by efforts to reduce bureaucracy and, in the U.K. and elsewhere, there are incentives and tax credits associated with investment in technologies that improve efficiency and generate jobs.

U.S. companies are investing in IT, but these dollars are being spent primarily on fundamental needs. Across industries, an average of 74 percent of the IT budget is spent on operational expenses or "keeping the lights on," i.e., maintaining legacy applications and infrastructure. This leaves only 26 percent of the average IT budget to be spent on implementing strategic business solutions such as new applications or IT infrastructure, according to one Gartner report.[6]

U.S. companies are somewhat more reactionary when it comes to IT investments. A greater percentage of U.S. companies invest due to system failures (nearly 40 percent as compared to 29 percent for non-U.S. firms) and internal problems that result in loss of profitability (30 percent and 22 percent, respectively) (Figure 2).

FIGURE 2. Factors that trigger a technology investment

Manufacturers based in the United States are investing at similar levels to non-U.S. manufacturers in enterprise networks, such as WAN and LAN. Overall, a majority of the participants in the Monitor have successfully implemented enterprise resource planning technology; about half of the participants enjoy some success in cloud computing, mobile technology, and big data and business analytics.

As noted earlier, a closer look at the degrees of successful implementation reveals some starker contrasts. While they are matching the investment levels of their offshore counterparts, U.S. manufacturers are doing so with less success.

U.S. COMPANIES BEHIND THE CURVE

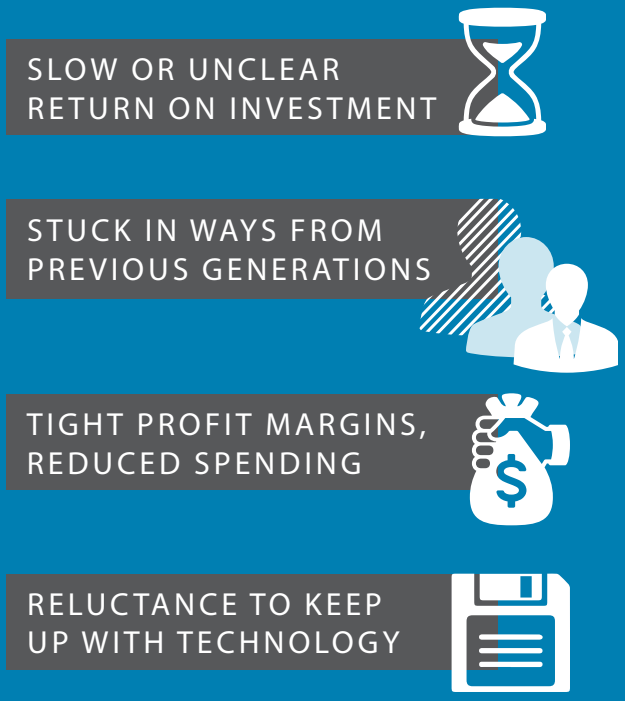
Why are U.S. companies behind in their utilization of IT?

It is worth noting that among those participating in the 2015 Monitor, overall business conditions were virtually identical across the board. That is, while sales and employment figures varied among companies, the aggregate in the United States and abroad had a similar percentage of thriving (36 percent), holding steady (56 percent) and declining (9 percent) companies. They have experienced healthy profits (a median of 8 percent for U.S. companies, 10 percent for non-U.S.) and expect strong profits in the coming year. This suggests that there are fundamental differences in business strategies at play.

According to the report by The Conference Board, manufacturing CEOs are "highly focused on innovation," making it a No. 1 priority for their organizations. Innovation certainly includes, but is not limited to, technology investments; implementation of these investments, however, follows hiring the workforce talent and cultivating a culture of innovation in their strategic plans. (*Also see separate report, McGladrey Monitor on Innovation.*)

The profile of these U.S. Monitor participants—particularly those earning gross revenues of less than $1 billion annually—may provide some insight into these strategies. They are primarily privately or closely held businesses (64 percent) engaged in labor- or equipment-intensive operations that generate most of their revenue domestically. They are keeping a close eye on their margins and, as such, may be reluctant to invest in areas where the return is not immediate or clear.

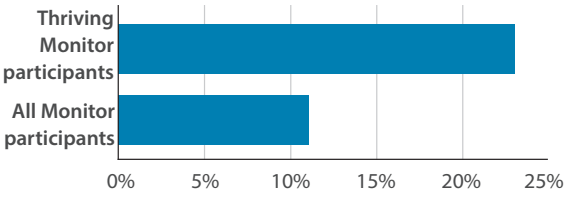
As *Forbes* magazine and others have noted, less than one-third of family businesses survive the transition from first to second generation ownership; even fewer survive the transition from second to third generation.[7] Those that are family owned may be rooted—some might say stuck—in traditions that are difficult to change. This may account in part for the reluctance to take a more progressive approach to technology and the preference to stick with maintaining what is already in place. Technology changes quickly and older generations may be reluctant to keep up with it.



Strategic IT investments contribute to growth

For manufacturers, the confidence in technology to provide improvements will vary, depending on a number of factors. When asked approximately what percentage of their investments in information technologies (such as IT infrastructure and business system hardware and software) will help them transform or materially improve their IT current capabilities (as compared to simply maintaining existing IT capabilities), up to one-quarter of IT investments are anticipated to provide improvements to more than half of Monitor participants overall (57 percent).

FIGURE 3. Percentage dedicating up to 50% of IT investments to improving capabilities



As business conditions improve, the percentage of IT investments dedicated to making improvements increases. For example, only 11 percent of Monitor participants overall dedicate up to 50 percent of technology investments to improve IT capabilities, compared to 23 percent of thriving companies (Figure 3).

Across the board, thriving companies anticipate median growth of 10 percent domestically, compared to a 4 percent median growth expected by companies that are holding steady and declining. These thriving companies also anticipate increasing their workforces by a median of 5 percent; the others anticipate their workforce changes to remain virtually flat. Notably, thriving companies anticipate increasing their IT investments by as much as 8 percent; holding steady and declining companies are expected to increase only by as little as 2 percent.

While it may be difficult to demonstrate direct causality between IT investments and revenue generation, the Monitor results suggest that companies continually investing in their technology environments can expect those investments to provide a return. "Systems that help management identify, understand and reach customers have a direct impact on revenue generation," says Bill Kracunas, a principal in McGladrey's technology and management consulting practice. Applications that enable efficiencies and provide supply chain data in real time will help address costs. Implementing and utilizing an up-to-date IT environment effectively can be an important element of strategic planning and a critical factor in a company's growth

The data security dichotomy

When it comes to their own companies, **many executives feel it unlikely their data will be a target** of any breach attempts.

When it comes to IT security, no company is immune to unauthorized access to its data. Recent high-profile data breaches have influenced U.S. companies to update their security protocols, according to a McGladrey Middle Market Leadership Council survey.[8] For Monitor participants, these updates include enhanced employee security protocols and new or upgraded software.

Yet when it comes to their own companies, many executives feel it unlikely their data will be a target of any breach attempts. They believe that their companies are too small or that their data is too insignificant or even useless outside the context of their business. Nevertheless, confidence lags behind for most Monitor participants—63 percent overall are only somewhat or not at all confident in their current ability to monitor and safeguard sensitive customer data from unauthorized access. These perceptions, and the security decisions that are informed by them, threaten to make companies vulnerable.

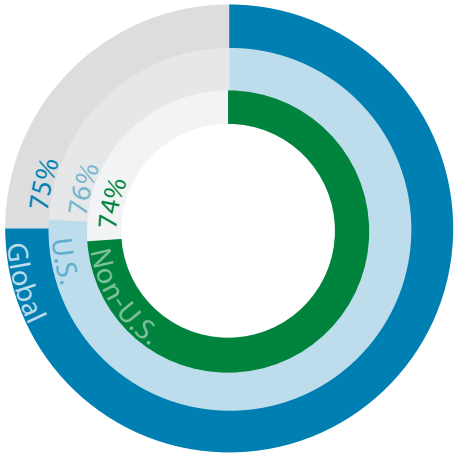
According to a study by Kaspersky Lab, manufacturers primarily fear losing client or customer information, followed by intellectual property; they are much less concerned with losing customer credit card information, personnel information or corporate bank account access.[9] But bank account information, for example, is particularly attractive to thieves, enabling them to transfer funds when a computer virus is introduced into a system used to manage the account.

In fact, many organizations are victims of cyberbribery, their systems brought down by "denial of service" attacks, followed by the attacker asking for a cash payment (in bit coins, for example) to bring the systems up again. In this regard, intellectual property notwithstanding, most businesses today are at risk.

Manufacturers and data security

In today's business and technology environment, all information has value. Hackers can attempt a large-scale strike to access credit card or health care information, and they can also attempt to steal bandwidth or email addresses—resources all companies possess. Monitor participants may be aware of this vulnerability intuitively: While three-quarters of them report that their companies have had no security breaches (Figure 4), more than 60 percent are only somewhat (or not at all) confident that they have the ability to monitor and safeguard sensitive customer data from unauthorized access.

FIGURE 4. Percentage reporting no security incident in the last 12 months



Most companies are lacking the basic tools to log and monitor the activity on their network infrastructure. They have invested heavily in the perimeter defenses to protect against attackers, but have not made the same investment in monitoring and logging infrastructures to help detect and contain data breaches. The leaders of these companies have not seen any evidence of a breach, but they lack the ability to verify that a data breach hasn't occurred, and this in part leads to their

apprehension. In the 2014 Monitor, it was noted that more than one-fourth of executives thought their systems were secure because "that's what I am told." Confidence in a company's security measures would rise with the greater certainty that monitoring technologies can bring.

This lesson has not been lost on companies based in China. Although the number of China-based companies participating in the Monitor is relatively small (37), they have the highest percentage of companies that are very confident in their IT departments' ability to safeguard data (67 percent). Companies in the United Kingdom come in at a distant second (45 percent). In Europe, the investment in security defenses and processes has increased rapidly over the last two years, which leads to heightened confidence. Moreover, the demand for audit and assurance services to provide a viewpoint on the strength of an organization's security control environment has also increased, leading to greater confidence and peace of mind.

The percentage of companies in the United States and Brazil that are very confident in their IT departments is even lower, at about 37 percent.

Because the United States has the largest economy in the world, U.S. companies comprise the largest corporate targets. Many U.S. laws require companies to disclose when a major data breach has occurred, something that is not required in other countries and is therefore difficult to measure. So the perception is that U.S. companies are more vulnerable than those in other countries. However, confidence that U.S. companies are more vulnerable than others is likely misplaced because it is based on a lack of data regarding the extent of data breaches outside the United States. "Attackers who are interested in monetizing stolen data are looking for the easiest targets and are not necessarily driven by geography," notes Sudhir Kondisetty, a principal in McGladrey's consulting services practice.

According to a Ponemon study, malicious or criminal attacks on organizations vary widely by country. Companies in Brazil and France are more likely to have a data breach involving a minimum of 10,000 records. In contrast, companies in Germany and Canada are least likely to have a breach.[10] The costs incurred vary widely, as well: The average per capita cost of a data breach is more expensive in the United States and Germany than in Brazil and India. Some may put these costs down as the price of doing business, but that is not a strategy for long-term survival.

Most common mitigation efforts may not be enough

President Barack Obama has said cybersecurity vulnerability will only get worse, and has called on Congress to pass a stronger legislation that would encourage private companies to voluntarily share information about cybersecurity attacks in an effort to prevent more breaches. Efforts to date, however, did not stop the data breach of some 4.2 million federal workers' personnel information reported in June of this year.

Perhaps the most effective action that any organization can take to reduce the risk of successful security attacks is **user education**.

FIGURE 5. Actions taken to enhance IT and data security

Despite the potential financial and reputational consequences, a survey in the United Kingdom of 400 executives found that one-third of them had no data breach response plans—and among firms with plans, 27 percent had no legal support in place.[11] This may be an example of executives thinking that data breaches happen mainly in the United States. and "not in my backyard."

Overall, U.S. and non-U.S. Monitor participants are taking many of the same security measures to guard against unauthorized data access (Figure 5), but to varying degrees, depending on business conditions. The primary action taken is to enhance employee security protocols (such as passwords), a relatively low-cost procedure but one that nearly 60 percent of thriving companies are taking as compared to only 39 percent of declining companies.

Moreover, password controls are relatively easy to bypass, and companies should incorporate efforts to improve their security infrastructure into their corporate strategic plans. This takes investments in time and money, which should be recognized by the executives leading the company.

Among the top five actions taken by Monitor participants overall, just over half of thriving companies purchase new or upgraded software while only 27 percent of declining companies will take this step.

"Perhaps the most effective action that any organization can take to reduce the risk of successful security attacks is user education," says Steven Snaith, partner and head of technology risk assurance at Baker Tilly Risk Advisory Services LLP. The most common form of cyberattack is through social engineering—that is, through contacting personnel by email or phone and duping them into disclosing confidential information that can subsequently be used to gain access to systems and data. Therefore, strong end-user awareness and education processes are critical actions to take to minimize this risk, supported by robust policies and procedures, password management, network security controls, encryption, removable media controls and monitoring controls.

Amid all of the efforts taken by companies to enhance IT and data security (and despite the many high-profile and expensive breaches of late), one in 10 companies participating in the Monitor say they are taking no actions to improve safeguards. With so much at stake—potential financial losses, compromised brand reputations, access to operational capital and possible regulatory violations—taking no action should not be an option.

Recognizing the shift

Companies that are not utilizing technology more strategically will not maintain a competitive edge, particularly in the U.S. market upon which so many businesses are setting their sights. U.S. manufacturers and distributors that want to compete in domestic as well as global markets need to take steps to successfully leverage technology:

Transform through IT

Technology is a conduit to a transformational process. "More companies now have a global footprint, and it is critical to access real-time information and create integrated workflow based on the business and not on product constraints," notes Steve Ems, a principal in McGladrey's consulting services practice. Systems now have sophisticated workflow capabilities that can be customized to an organization's business model and bring efficiencies to their processes. Collaboration and innovation technologies are more widespread, eliminating barriers for organizations and changing how they go to market.

Manufacturers and distributors need to invest in solutions that may well revolutionize their entire technology platform. Customer expectations have changed, and organizations must update their infrastructure and systems or risk being left behind.

With so much riding on how IT is utilized—providing products and services, increasing efficiencies, optimizing product usage, customizing client engagement—management at U.S.-based companies must allow IT leaders to play a primary role in the strategic direction of the company, because non-U.S. companies are making significant investments that are helping drive their success.

Enhance data security

As hackers become more advanced, organizations must increase their focus on cybersecurity to protect sensitive data and systems. No organization, regardless of size or industry, is immune to cyberattacks, and just one breach could cause significant financial, reputational or regulatory consequences. Manufacturing is among the top targets and one company's Internet footprint looks the same as another to anyone interested in finding something of value, whether it's credit information, personnel information, intellectual property (such as engineering drawings or processes), technology or other assets. These hackers are sophisticated, educated computer experts employed by corporations, organized crime, terror organizations and governments with significant resources.

An effective control environment, however, can reduce the likelihood of a breach, enhance incident detection and response, and accelerate recovery efforts to limit damage.

Although companies should not neglect the perimeter security infrastructure components designed to prevent security breaches, they need to understand there is always a chance that a breach will occur. Organizations need to focus their time and money on these monitoring, detection and remediation controls as well. Organizations that follow best practices build strong infrastructure components and business processes to detect a breach, contain the breach and quickly respond to the ramifications of the breach.

While larger companies may be able to absorb the initial costs associated with a breach, the impact of hacker activity may be felt by companies as well as their employees and clients for quite some time. Breaches that target private information can leave a reputation in tatters and open a firm up to legal ramifications. Lost business resulting from a breach has potentially even greater financial consequences.

Taking a systematic approach to understanding, managing and monitoring risks to an organization can give management better insight into company operations and may even allow the company to turn certain risks into opportunities. And with the rise in information breaches, keeping data secure can be a competitive edge.

Information technology **and data security** TAKEAWAYS

TRANSFORM THROUGH TECHNOLOGY

Find and invest in technology

Manufacturers and distributors need to invest in solutions that may well **REVOLUTIONIZE THEIR ENTIRE TECHNOLOGY PLATFORM**.

Non-U.S. companies invest more diversely and successfully

IT investments made by non-U.S. companies show **MORE DIVERSITY** and are achieving a greater percentage of **SUCCESSFUL IMPLEMENTATION** than investments made by U.S. companies.

Update or be left behind

Organizations must **UPDATE THEIR INFRASTRUCTURE AND SYSTEMS** or risk being left behind.

IT leaders should help lead the company

IT leaders should play a **PRIMARY ROLE IN THE STRATEGIC DIRECTION** of the company.

ENHANCE DATA SECURITY

No one is immune, protect yourself

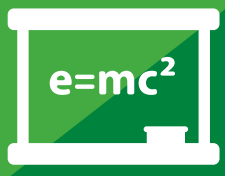
No organization, regardless of size or industry, is **IMMUNE TO CYBERATTACKS.** Every organization should **PROTECT THEMSELVES.**

It only takes one!

Just one breach could cause **SIGNIFICANT FINANCIAL, REPUTATIONAL OR REGULATORY CONSEQUENCES.**

Build strong infrastructure

Build strong infrastructure components and business processes to **DETECT, CONTAIN AND QUICKLY RESPOND** to the ramifications of a breach.



User education is key

The **MOST EFFECTIVE ACTION** that any organization can take to reduce the risk of successful security attacks is **USER EDUCATION**.

Acknowledgements

Methodology

The 2015 McGladrey Manufacturing & Distribution Monitor was conducted using an online questionnaire promoted by McGladrey, industry associations, and a research panel organization to manufacturing and distribution companies. There were 1,660 total valid respondents to the 2015 Monitor survey, with completed questionnaires received in March and April 2015. Responses were received by The MPI Group, an independent research firm, and then entered into a database, edited and cleansed where necessary to ensure answers were plausible. All respondent answers to the 2015 McGladrey Manufacturing & Distribution Monitor are confidential. As an incentive to complete the study, participants that provided contact information are being provided a customized benchmark report.

2015 Manufacturing & Distribution Monitor series

The 2015 Monitor is a series of reports on issues of concern for the manufacturing and distribution industries. Topics in this series include: global growth, investing for growth and innovation, and information technology and data security. The reports are available online at www.mcgladrey.com or through your local McGladrey representative.

Focus group insights

Many thanks to the following focus group participants for their time and insights:

- Frank Barnett, Vice President, Finance, Nutramax Laboratories, Inc.
- Mark Holzman, Chief Financial Officer, Saval Foods Corporation
- Gary Kratchovil, Executive Vice President of Operations, Citrus and Allied Essences
- Kevin Monaco, President, Turf Equipment

2015 Manufacturing & Distribution Executive Summits

Nearly 1,000 manufacturing and distribution professionals participated in the McGladrey Manufacturing & Distribution Executive Summits held throughout the country in the fall of 2014. Contact your local McGladrey office or go to www.mcgladrey.com/industrialproducts for details on the 2015 Summits and to learn about our other industry events, resources and services.

Subject matter specialists

Steve Ems *Principal, Consulting Services,* McGladrey LLP	steve.ems@mcgladrey.com	856.722.1787	Moorestown, N.J. USA
Alfonso Elías Bornacini *President of the Board of Members,* RSM Mexico	alfonso.elias@rsmi.com.mx	(52) 55 5093 6200	Mexico City, Mexico
Jake DeWoskin, *Director, Technology and Management Consulting,* McGladrey LLP	jake.dewoskin@mcgladrey.com	612.376.9302	Minneapolis, Minn. USA
Wesley Montechiari Figueira *Senior Partner,* RSM Brasil	wesley.figueira@rsmbrasil.com.br	(55) 41 3015 5888	Curitiba, Brazil
Sudhir Kondisetty *Principal, Consulting Services,* McGladrey LLP	sudhir.kondisetty@mcgladrey.com	215.648.3121	Blue Bell, Pa. USA
Chris Knowles *Partner, Head of Technology Consulting,* Baker Tilly Consulting LLP	chris.knowles@bakertilly.co.uk	44 (0)20 3201 8000	London, United Kingdom
Bill Kracunas *Principal, Technology and Management Consulting,* McGladrey LLP	bill.kracunas@mcgladrey.com	617.241.1331	Boston, Mass. USA
Karen L. Kurek *Partner, Industrial Products,* McGladrey LLP	karen.kurek@mcgladrey.com	312.634.3920	Chicago, Ill. USA
Rodolfo Martínez Septién *Board of Members,* RSM Mexico	rodolfo.martinez.septien@rsmi.com.mx	52 (999) 925 6680	Mérida City, Yucatán, Mexico
Steven Snaith *Partner, Head of Technology Risk Assurance,* Baker Tilly Risk Advisory Services LLP	steven.snaith@bakertilly.co.uk	44 (0)20 3201 8000	London, United Kingdom
Chris Wetmore *Director, Consulting Services,* McGladrey LLP	chris.wetmore@mcgladrey.com	617.241.4656	Boston, Mass USA

Production

Terri Andrews, *Director*	Public relations
María Virginia Bernardini, *Director, Communication Specialist*	Bernardini Asociados
Sophia Boutalbi, *Marketing and Business Development Executive*	Baker Tilly Tax and Accounting Limited
Sandra Clark, *Content Proofer*	Proofreading
Stacey Doherty, *Director*	Marketing
Ken Foster, *Director*	Digital media
Kristen Harvey, *Manager*	Graphic design
Jenna Huntley, *Designer*	Graphic design
Tracie Lopes, *Manager*	Marketing
Steve Magnino, *Director*	Market research
Frank McGee, *Manager*	Editor-in-chief
Dan O'Shea, *Manager*	Writer
Brett Pyrtle, *Principal, Turning Point Communications LLC*	Writer
Melissa Toledo, *Senior Director*	Marketing research and strategy

References

1. Coy, P. "The Bloomberg Innovation Index" (2015).
2. Guevara, JK et al, "IT Key Metrics Data 2014: Key Industry Measures: Cross Industry Analysis: Multiyear" (December 2013) Gartner.
3. "Quarterly Retail E-Commerce Sales, 4th Quarter 2014" (Feb. 17, 2015), U.S. Department of Commerce.
4. Mitchell, C. et al "CEO Challenge® 2015" The Conference Board.
5. "Sanctions for data breaches" (Aug. 1, 2014) # 5-518-8056, Practical Law.
6. "IT Key Metrics Data: 2012 IT Enterprise Summary Report" (December 2013) Gartner.
7. "The Facts Of Family Business" (July 31, 2013) Forbes.com.
8. "The Real Economy, Vol. 4" (April 2015) McGladrey LLP.
9. "Global IT Security Risks 2014—Online Financial Fraud Prevention" Kaspersky Lab.
10. "2015 Cost of Data Breach Study: Global Analysis" (May 2015) Ponemon Institute LLC.
11. Summerfield, R. "Reacting to data breach litigation" (June 2015) Financier Worldwide.

Power comes from being understood.®

When you trust the advice you're getting, you know your next move is the right move. That's what you can expect from McGladrey. That's the power of being understood.

800.274.3978
www.mcgladrey.com

McGladrey

SV-NT-ALL-ALL-0715