THE MPI INTERNET OF THINGS STUDY

SPONSORED BY BDO

APRIL 2017

> “No manufacturer, regardless of size or ingenuity, is immune to technology disruption. The question companies need to ask themselves isn’t whether they can afford to invest in the future of manufacturing; it’s whether they can afford *not* to.”

Rick Schreiber, partner and national leader of BDO’s Manufacturing & Distribution practice

Manufacturers Weigh Risks & Rewards for IoT Opportunity

MANUFACTURING IS GETTING A REBOOT. ARE YOU READY FOR THE REVOLUTION?

The Internet of Things. Industry 4.0. The digital industrial. Whatever you call it, one thing is clear: The next era of manufacturing is here.

The MPI Internet of Things Study, sponsored by BDO, finds that manufacturers are making headway toward embracing the IoT and improving their readiness—more than half (51 percent), in fact, characterize themselves as IoT-competitive companies, and another 14 percent say they're IoT leaders. But they still have a long road ahead of them and face big obstacles along the way.

Uncertain if the opportunity is worth the investment? Seventy-two percent of manufacturers report the application of the IoT to their plants and processes resulted in an increase in productivity in the last year, while 69 percent report seeing an increase in profitability, with 12 percent reporting increases of more than 10 percent.

Looking forward, 60 percent of manufacturers have a strategy in place to apply the IoT to their processes—and 36 percent are already implementing it. If you're among the 40 percent without an IoT strategy, now is the time to develop a plan and put it in action. And for those with a plan already underway, don't forget about risk while chasing opportunity. Data exclusive to BDO finds two critical components of IoT strategy that manufacturers are underestimating: cybersecurity and research and development (R&D) credits.

The MPI Internet of Things Study, conducted by The MPI Group and sponsored by BDO and SAS, evaluated the readiness of global manufacturers to incorporate smart devices and embedded intelligence within their plants and into their companies' products. In November and December 2016, 374 manufacturers participated in the study.

72%

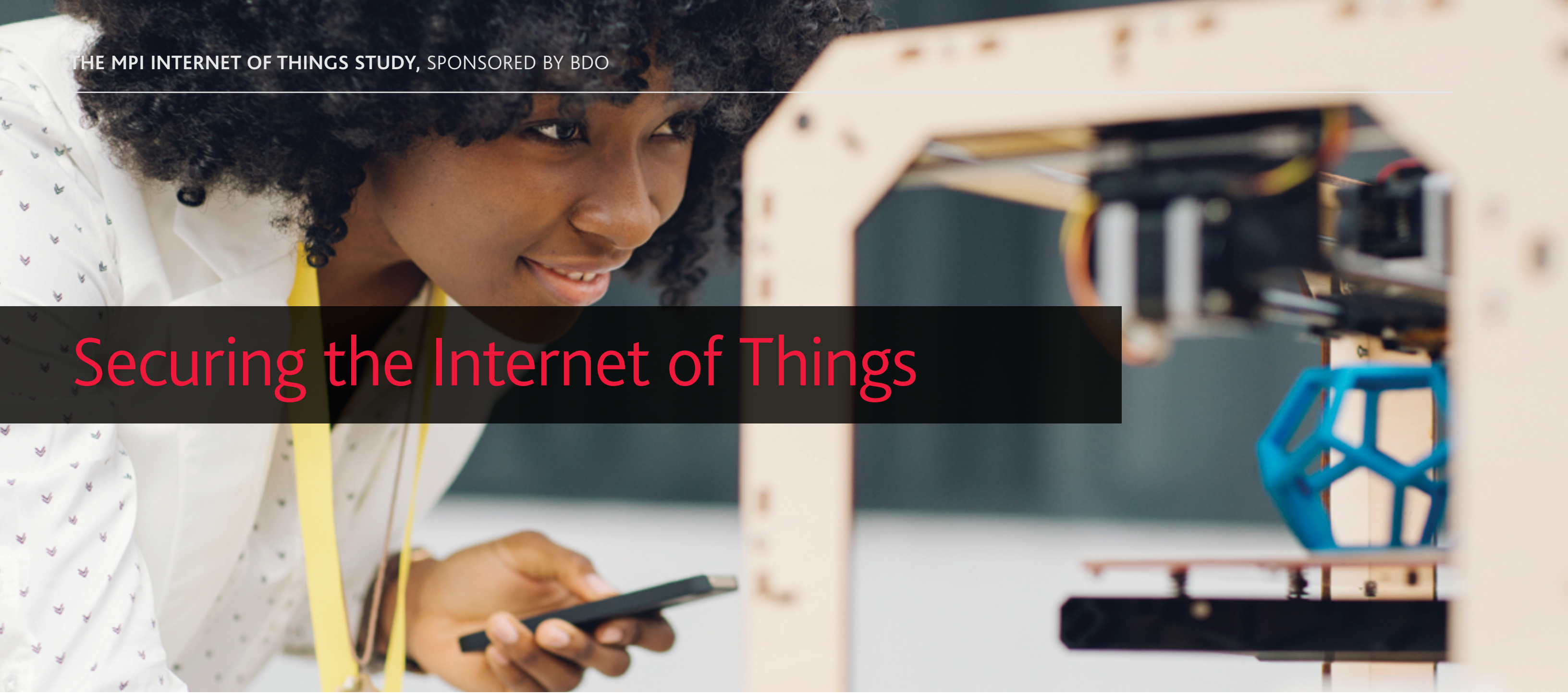
of manufacturers increased their productivity in the last year by applying the IoT to their plants and processes.

69%

of manufacturers increased their profitability in the last year by applying the IoT to their plants and processes.

1/2

of plant production equipment and processes are *currently* managed via the IoT—with 88% expecting to increase their application of the IoT in the next two years.



Securing the Internet of Things

In our *2016 Manufacturing RiskFactor Report* analyzing the risk factors cited in the 100 largest publicly traded U.S. manufacturers' annual filings, we reported that cyber risk ranked in the top 10 risk factors for the first time in our study's history. More than 9 in 10 manufacturers (92 percent) cited cybersecurity concerns in 2016, up a staggering 44 percent from 2013.

Cyber is finally on manufacturers' radars—and not a moment too soon, as the IoT introduces a host of new cyber threats and attack vectors for bad actors. Last September, the Mirai botnet, a strain of malware that infects internet-connected devices and corrals them into an IoT "army" to overwhelm a target's servers with malicious traffic, made headlines for triggering a massive internet outage. The original Mirai botnet counted approximately 500,000 IoT devices worldwide. Following the attack, the manufacturer of the devices used to make Mirai was forced to issue a recall.

Mirai remains a real threat—not only for manufacturers of IoT devices, but also for any organization that leverages the IoT. On October 1, 2016, the hacker behind the botnet, known as "Anna-senpai," subsequently open-sourced its code, enabling fellow hackers to develop their own Mirai strains to target additional IoT devices and increase the botnet's compute power. And while Mirai is currently the star of the show, it's far from the only game in town. The Leet Botnet, which came onto the scene at the end of 2016, is rumored to rival Mirai in its capacity to do damage.

Despite the acceleration of IoT-powered attacks, 81 percent of survey respondents say they are confident or very confident in their current cyber risk management program to address the IoT environment. Just under a fifth (19 percent) are unsure or not confident in their current program to address security concerns in the IoT. Given the magnitude of recent IoT-enabled cyberattacks, manufacturers' level of cyber confidence is surprising—and potentially worrisome.

Manufacturers may feel that the innovation rewards of the IoT are not worth the cyber risk. But there is no escaping the IoT; it's already here. If your employees bring their personal devices into the workplace or use them to remotely check work email, your corporate network is exposed to the IoT. Two-thirds of manufacturers either allow or are considering allowing non-corporate devices into plants. However, only a third have implemented Bring Your Own Device (BYOD) policies and procedures.

92%

of manufacturers rank cyber risk as a top risk factor for their business.

Many manufacturers prioritize continuity over innovation because any downtime of systems can disrupt revenue. Forty percent of manufacturers surveyed cite adapting existing technologies as one of the biggest challenges to implementing the IoT. But relying on legacy infrastructure, which can include outdated PCs and equipment, can inadvertently expose manufacturers to risk. Legacy systems are inherently tough to secure against modern cyberthreats, and it can be difficult to connect and service disparate systems.

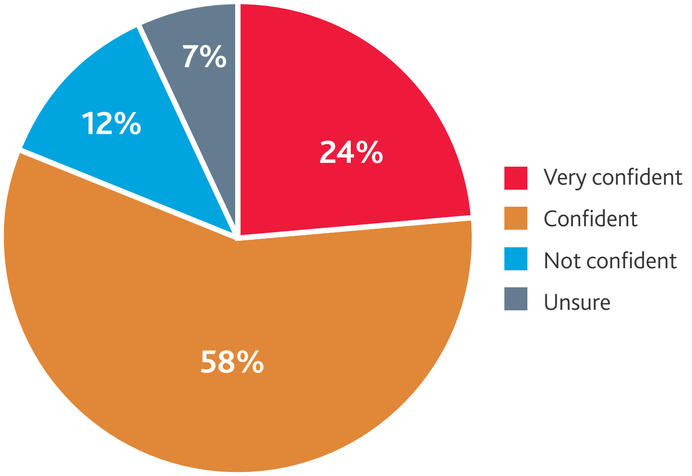
> "A data breach can result in angry customers and lost business, particularly if the victim company is deemed cyber-negligent. And for manufacturers that sell to highly regulated industries or the government, an insufficient cyber posture—even if they haven't had a data breach—can knock them out of the running for new business or result in terminated contracts."

Shahryar Shaghaghi, Technology Advisory Services national leader and head of International BDO Cybersecurity

Third-party cyber risk also increases exponentially with the IoT. If we look back at the Mirai botnet incident, the primary target was Dyn, a cloud-based Internet Performance Management company that controls a substantial portion of the internet's domain name system infrastructure. But when Dyn's servers went down, it wasn't the only victim—the websites of its 3,500-plus enterprise customers also went down.

The saying "you're only as strong as your weakest link" rings true for cybersecurity in an IoT environment. Sophisticated attackers frequently exploit third-party vulnerabilities to gain access to their ultimate target. Any security gaps in manufacturers' supplier networks can serve as ingress points for hackers. While most manufacturers are cognizant of and actively address third-party cyber risk, more than a quarter (27 percent) do not have or are not sure if they have a security policy in place for their supply chain partners and other vendors. On the flip side, manufacturers can also be the ingress point for hackers to reach their supply chain partners and end-customers.

HOW CONFIDENT ARE YOU IN YOUR ORGANIZATION'S CURRENT CYBER RISK MANAGEMENT PROGRAM TO ADDRESS THE IOT ENVIRONMENT?



In this high-risk environment, manufacturers can't afford to make cybersecurity an afterthought—and a good number are not. Nearly half (47 percent) of manufacturers surveyed start thinking about cybersecurity considerations during the product conceptualization and design stage—which, in our view, is when cyber needs to come into the picture. And we're not alone in our thinking: In November 2016, the Department of Homeland Security issued six strategic cybersecurity principles for the IoT. "Incorporate security in the design phase" is the first principle on their list.

Less ideal, 21 percent of manufacturers start thinking about cybersecurity during the production stage, while another 18 percent hold off until the quality control phase. Nine percent either don't start weighing cyber considerations until they're marketing the product (when it is typically too late to make significant changes) or don't consider cybersecurity at all.

23%

of manufacturers don't consider cybersecurity until the quality control or marketing stage of the manufacturing process.

R&D Tax Credits Fly Under the Radar

One of the biggest hurdles to embracing technological change—including the IoT and beyond—is figuring out how to pay for it: 31 percent of surveyed manufacturers rank budget and resources as their biggest challenges to applying IoT capabilities.

Yet, while 79 percent of manufacturers say they are investing in the IoT, only 43 percent are planning to claim IoT-related tax credits and investments. The rest may be leaving money on the table.

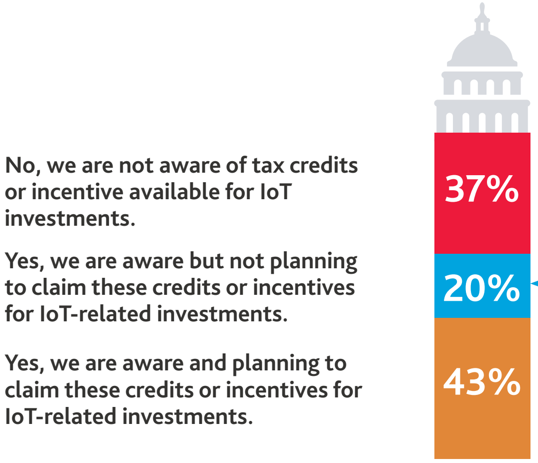
Last year, over 6,000 manufacturers claimed an estimated $10 billion in R&D tax credits, with each manufacturer's average benefit exceeding $1 million. But that number could be much higher.

Designed to encourage investment in innovation, R&D tax credits offer manufacturers significant benefits, equaling up to an average of 10 percent of qualified spending. In general, federal and state R&D credits are available to businesses that attempt to develop or improve the functionality or performance of a product, process, software or other component using engineering or the physical, biological, or computer sciences to evaluate alternatives and eliminate uncertainty regarding the business' capability or method to develop or improve the component or the component's appropriate design. In addition, more than 35 countries offer often more generous incentives for similar activities and investments.

57%

of manufacturers are not planning to claim tax credits and incentives available for IoT investments.

AWARENESS AND PLANS TO CLAIM FEDERAL, STATE AND NON-U.S. TAX CREDITS AND INCENTIVES AVAILABLE FOR IOT INVESTMENTS (% OF PARTICIPANTS)



REASONS COMPANIES ARE NOT PLANNING TO CLAIM CREDITS AND INCENTIVES:

	% of respondents
Expected benefit too small	25%
Expected cost to claim too high	23%
Not enough documentation to support claim	18%
Our activities don't qualify	16%
Expected ROI would be immaterial	13%
Other	25%

"The objective of R&D credits and incentives is to incentivize exactly the type of progress manufacturers are trying to achieve. Qualifying activities don't need to be flashy or revolutionary, or even succeed. If you're trying to make products, processes or software better, faster, cheaper or greener, you probably qualify."

Chris Bard, tax partner and R&D practice leader at BDO

In December 2015, the Protecting Americans from Tax Hikes Act (PATH Act) expanded and made permanent the federal R&D tax credit, thus putting an end to its tumultuous history of repeated expirations and renewals at the eleventh hour. In addition to expanding the credit to benefit startups and small businesses, this allowed tax executives to include the credit in their long-term business planning without concerns about expiration.

Still, a little more than a year after the PATH Act went into effect, more than half (57 percent) of manufacturers are not planning to claim tax credits and incentives for their IoT investments. More than a third (37 percent) aren't aware R&D credits are available to them.

For the 20 percent of those surveyed that are aware of R&D credits but are not planning to claim them, a quarter (25 percent) believe the expected benefit is too small, while another 23 percent expressed concern about the cost to claim the credit.

Notably, the percentage of respondents not claiming R&D credits because they don't believe they are doing any qualified activities dropped significantly year-over-year, shrinking from 24 percent to 16 percent. It is important to note that most R&D credits don't require activity to be groundbreaking to qualify, or even that the activity succeed.

> "The reality is that most manufacturers are still struggling with the transition to Industry 4.0. Many are still relying on legacy infrastructure that can't integrate with IoT devices and applications or modern security protocols. The factory of the future must be built on a sound foundation."

Eskander Yavar, partner and national leader of BDO's Management Advisory Services practice

In our view, the IoT is just the tip of the spear. It's what manufacturers will be able to do with a whole new layer of data—transmitted and received in real time via wireless and sensor-enabled systems—that will revolutionize the way products are made and sold. Combining data-driven insights with the technology manufacturers can now deploy on factory floors—in the products they design and across the supply chain—is set to spur a manufacturing renaissance. But starting on the path to transformation is easier said than done, especially when it's new terrain.

Meaningful progress and innovation start with a comprehensive plan that considers both risks and opportunities. The winners of the fourth industrial revolution will be those that think about tomorrow, today.

About BDO's Manufacturing & Distribution practice

BDO has been a valued business advisor to manufacturing and distribution companies for more than 100 years. We work with a variety companies from all industrial sectors, ranging from global distributors to startup and niche manufacturing corporations, on a myriad of accounting, consulting, tax and other financial issues.

About BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 67,700 people working out of 1,400 offices across 158 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

For more information on BDO USA's service offerings to this industry, please contact one of the following practice leaders:

RICK SCHREIBER
National Manufacturing & Distribution
Practice Leader, Memphis
901-680-7607 / rschreiber@bdo.com

SHAHRYAR SHAGHAGHI
National Leader, Technology Advisory
Services, New York
212-885-8453 /sshaghaghi@bdo.com

CHRIS BARD
R&D Tax Practice Leader, Los Angeles
310-557-7525 / cbard@bdo.com

LARRY BARGER
Assurance Senior Director, Pittsburgh
412-434-8203 / lbarger@bdo.com

CATHY ROZANSKI MCNAMARA
Assurance Partner, Detroit
248-244-6524 / crozanski@bdo.com

ESKANDER YAVAR
Management Advisory Services National
Leader, Houston
713-407-3293 / eyavar@bdo.com

CONTACT US:

FIRST NAME

LAST NAME

EMAIL

PHONE

SUBJECT

MESSAGE

SUBMIT