

The Value of Mobile Devices for the IoT



The Internet of Things (IoT) is taking the business world by storm as companies increasingly rely on data from devices at the edges of their networks to gather business and customer intelligence. Among many other benefits, insights gathered from IoT data help business leaders identify shifting market trends, meet customer demands, increase operational efficiencies, and develop smarter, data-driven strategies.

This worldwide trend impacts businesses of all sizes across multiple industries. Research by global management consulting firm McKinsey & Company showed that well over half—62%—of senior managers expect the impact of the IoT on their companies to be “very high” or “transformative.”

At the same time, as more employees work away from traditional office environments and conduct business in the field, many of them are directly interacting with and gathering data from IoT systems with the help of mobile devices.

IDG and Panasonic recently surveyed 61 business leaders and IT decision makers who rely on mobile devices outside of traditional office settings, mainly in industries like manufacturing, healthcare, and transportation. More than three quarters of them say that their mobile workforce acts as an interface for the IoT through their laptops, tablets, and smartphones.

For these organizations and many others, mobile devices are a key part of their IoT strategy and overall digital transformation. These companies depend on the intelligence gathered through mobile devices to bring new insights about their customers and their operations—and those insights will determine the future of their company’s growth and well-being.

Mobile Device Data Drives Business Decisions

As organizations gather and analyze data from mobile devices as part of an IoT initiative, they discover actionable business intelligence that can be translated into immediate, measurable business benefits—like increased productivity in the workforce, according to 78% of respondents to the IDG/Panasonic survey.

Many businesses rely on that same data to inform long-term business strategies as well, leading to more efficient, decisive, proactive organizations. An equal amount of respondents—78%—are experiencing improvements in corporate decision-making as a result of mobile device data. Exactly three quarters say that they rely on data from mobile devices to develop new strategies or approaches. And 63% say they use mobile device data to enable a more predictive approach to maintenance and repair.

Perhaps most tellingly of all, 84% of business leaders surveyed say that their companies rely on data captured by mobile devices in the field for business benefit to a “large” or “very large extent.” This overwhelming majority clearly illustrates how integral mobile devices and the mobile workforce are in the development of the modern, digital, data-driven enterprise. But the transformative insights culled from mobile device data come with a catch.

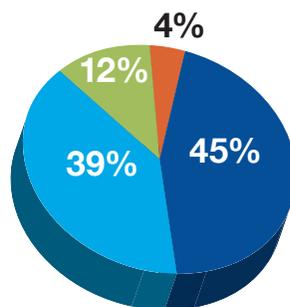
Devices in the Field Present New Challenges

Now more than ever, companies rely on mobile devices to rise to the challenge of operating reliably and securely in a variety of not-so-friendly conditions and environments—not only to enable

SPONSORED BY:

Panasonic

Reliance on Data Captured from Mobile Devices in the Field for Business Benefit



■ To a very large extent ■ To a large extent ■ To some extent ■ To little extent

employees to do their jobs, but also to deliver the vital insights that companies need in order to thrive.

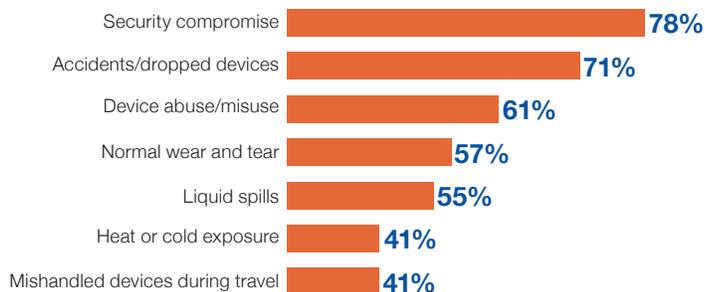
While businesses increasingly rely on mobile devices as “human interfaces” to the IoT—as more than 76% of IDG survey respondents report doing—concerns about cybersecurity and physical risks are top of mind.

And as collected data becomes more valuable—not only to companies collecting it, but also to competitors and hackers—the importance of protecting that data rises. For this reason, the great majority of IDG/Panasonic survey respondents—78%—report being concerned about data on mobile devices being compromised.

Concern about the physical dangers confronted by mobile devices is almost as high. After all, even in environments in which the cybersecurity risk is minimized, there exists the omnipresent danger of real-world damage to devices that are taken out of the office and into the field. The fear is not unfounded; damaged or destroyed devices may lose data that is more valuable than the devices themselves.

That’s why in the IDG/Panasonic survey, 71% of respondents are concerned about the risk of drops or other accidents to mobile devices. More than half—55%—are concerned about liquid spills, and 41% report concern about damage to devices caused by extreme temperatures. As the mobile and remote workforce continues to expand beyond the boundaries of traditional, controlled workspaces, these concerns are only escalating.

Risk of Using Mobile Devices in the Field as a “Human Interface” to IoT



Source: IDG Research

Well over three quarters—80%—of business leaders say they value security features such as hardware encryption and removable drives as their top “must-haves” for mobile devices. More than half—63%—name durable exteriors as their top consideration when purchasing mobile devices.

Mitigating the Mobile Risks

Fortunately, rugged mobile devices with robust security features can address the twin concerns of cybersecurity and physical risk reported by companies that rely on data collection by employees in the field.

Well over three quarters—80%—of business leaders say they value security features such as hardware encryption and removable drives as their top “must-haves” for mobile devices. More than half—63%—name durable exteriors as their top consideration when purchasing mobile devices. Rugged cameras, bar code readers, a variety of size and weight options, and a choice of screen types—including detachable and reconfigurable screens—also rate highly, with 51% of respondents rating each of these features as “must-haves.”

Organizations that effectively leverage the IoT are reaping the rewards, but continuing to do so effectively requires the right tools. For many organizations, that means equipping their employees who work in the field with rugged mobile devices that include built-in, state-of-the-art security features as a key part of their IoT strategy. Such devices may include weatherproof exteriors, tolerance to heat and cold, the ability to survive falls, glove-sensitive touchscreens, and more.

Visit panasonic.com/toughbook to learn how rugged and secure mobile devices can help companies meet the challenge of collecting data in the field.