WHITE PAPER

Low-Cost Computers Come at a Price

Why government organizations need ruggedized hardware

In a recent report on Mobile Computing, the International Association of Chiefs of Police states,

> *"It is remarkable how much benefit a law enforcement agency and consequently the public can experience from a successful mobile computing system … [T]he percentage of savings in time, personnel, money, consumables, accuracy, and safety can be truly monumental, often between 20-40 percent."*[1]

Notebook Five-Year TCO:

Rugged:	*$15,700*
Consumer:	*$27,100*

To realize the phenomenal benefits of mobile computing, equipment needs to be well-designed, user-friendly, and reliable—terms that, in the field of public safety and government services have definitions very different from their equivalents in consumer and office markets. Just as the family minivan isn't suitable for patrol duty, consumer- and office-grade mobile computers are a poor fit for situations faced by government workers in the field.

The temptation to purchase consumer-grade hardware for mission-critical applications is always there, particularly in lean times. After all, the purchase price is significantly lower, the hardware lighter and prettier, the brands familiar—and isn't one laptop the same as another? But in the unforgiving environments and urgent work faced by public safety and government personnel, "low-cost" consumer hardware turns out to be very costly.

A 2007 VDC Research Group study quantified the total cost of owning and supporting a mobile computing device for five years. In government applications, the cost differences were stark: a fully rugged notebook computer costs $15,700 to purchase, support, and operate—while a "low-cost" consumer laptop costs over $27,100 over the same time frame. Similarly, a "low-cost" consumer handheld PDA costs nearly $25,300 over five years—over $10,000 more than a fully rugged PDA.

These costs mean that each "low-cost" device—laptop or PDA—carries an extra cost of over $2,000 a year. In a department with as few as 40-50 employees, the savings from deploying ruggedized hardware can exceed $100,000 a year: enough to hire additional staff.

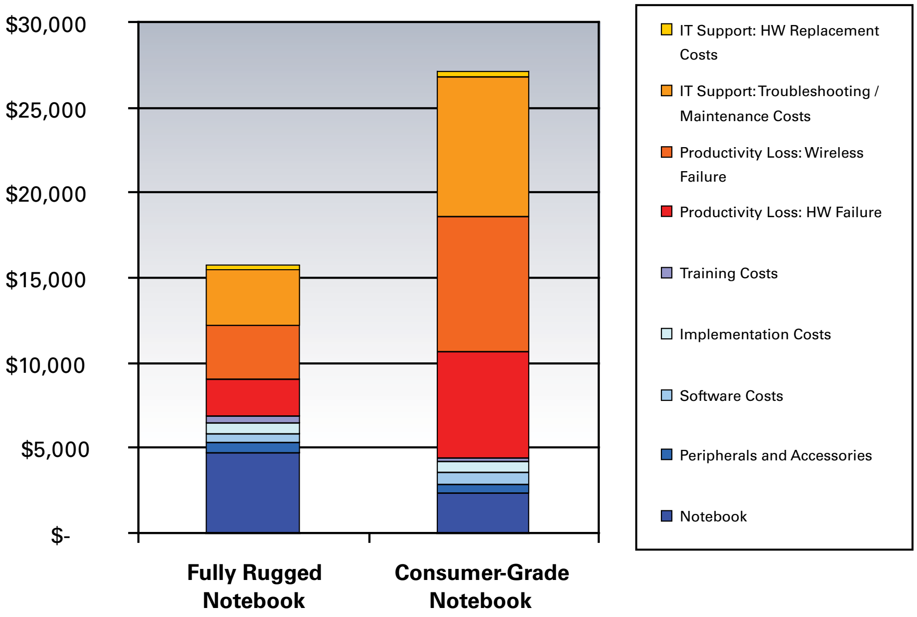
Why so expensive?

Even people familiar with the concept of TCO—Total Cost of Ownership, i.e. the amount of money spent on acquiring, maintaining, supporting, and use of a device—may be surprised at the magnitude of these numbers. It's one thing to understand that "computers cost money"; quite another to see how the purchase price of a computer is exceeded by the outlays required to support and keep it running. Then there is the cost of lost productivity, which is more difficult to measure, but no less real. After all, you bought the computer to realize "savings in time, personnel, money, consumables, accuracy, and safety." If it's not working, those savings are lost.

Consider, for example, the cost of failure of a laptop's hard drive—a crucial and vulnerable component that is left unprotected in most consumer hardware. The drive itself must be replaced, of course, which costs money—but that's only the beginning. If the drive fails in the field, the user has to fall back to pen-and-paper and diminished operation, or in the worst case, stop work and return to headquarters so the problem can be dealt with. Data that resided on the hard drive—whether un-filed reports, unsent emails, evidentiary photographs, or just notes—will either be lost, or require very expensive and uncertain recovery efforts. The new hard drive must be installed, with the operating system, applications, and security software configured and tested—increasing IT costs. At this point, the total IT costs and loss of productivity are likely to exceed any costs savings from having bought a "low-cost" consumer device. There are steps to mitigate the risk —frequent backups and spare hardware—but those also carry costs, and are no help against the loss of productivity in the field.

[1] "Mobile Computing Technologies," IACP Technology Desk Reference, p. 135, International Association of Chiefs of Police, 2006.

TCO Comparison (5-year) for Notebook Computers: Government Environments[2]



Annual Notebook Failure Rates:

Rugged: ***9%***

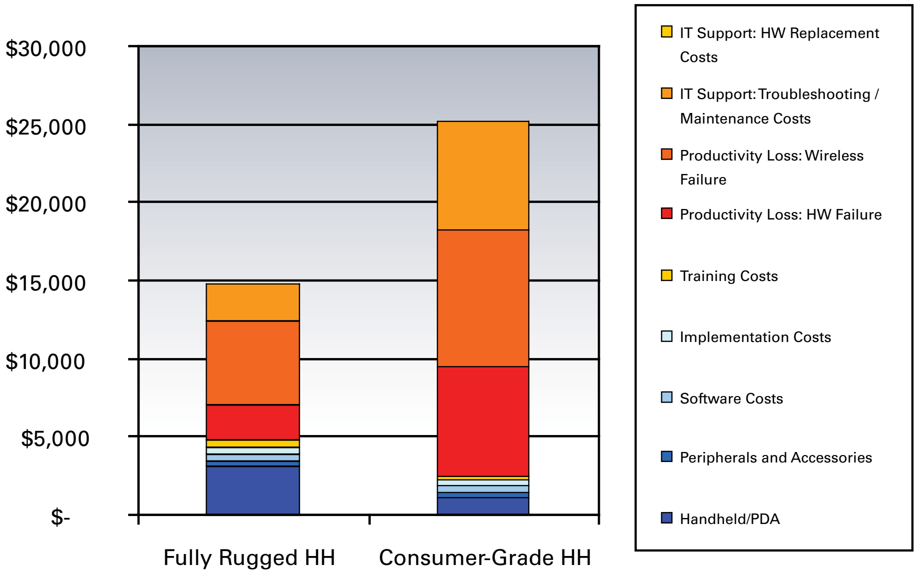
Consumer-grade: ***33%***

These costs are likely to show up surprisingly fast in consumer-grade devices. VDC reports that non-rugged computers have an annual failure rate of 33%—that is, in any one year, one out of three computers owned by an organization will require some kind of repair. By contrast, fully rugged devices suffer an annual failure rate of only 9%, resulting not only in lower repair and IT costs, but substantially higher productivity amongst staff using them.

VDC also reports that "the failure rate of non-rugged notebooks increases substantially with time," with annual rates in the first year being 15-20%, rising to 35% after the second year. By contrast, failure rates of rugged equipment remain "fairly consistent" over their installed life.

Looking at handheld computers, the contrast is equally stark. A consumer-grade device may be "cheaper" to purchase, but support and productivity costs quickly overwhelm any price advantage.

TCO Comparison (5-year) for Handheld Computers: Government Environments[2]



[2] "Government TCO Analysis," Total Cost of Ownership Models for Mobile Computing and Communications Platforms, pp. 278-279, VDC Research Group, 2007

A Failure To Communicate

One of the most valuable features of a mobile computer—whether notebook or handheld—is the ability to communicate over wireless data networks. This is particularly true in public safety, which has used mobile data terminals for decades. Wireless communication is one of the key generators of efficiency and productivity associated with mobile computing.

When it comes to wireless communications, consumer-grade devices turn out to be particularly vulnerable. Most only come equipped with WiFi built-in; some include Bluetooth. This, however, is insufficient for mobile workers, who require access to wide-area networks—whether private data networks or public cellular networks. To get around this shortcoming, workers end up plugging in external cards, which are more vulnerable to breakage and give inferior performance. As VDC states in their report,

> *"For each wireless connection dropped during transmission, users experience anywhere from 5-10 minutes of lost productivity (need to re-logon to VPN, etc.). These interruptions can quickly add up to significant operational costs, not to mention frustrated employees. It is well documented that wireless radios that are integrated in the mobile device generally achieve superior performance when compared to plug-in solutions."*[3]

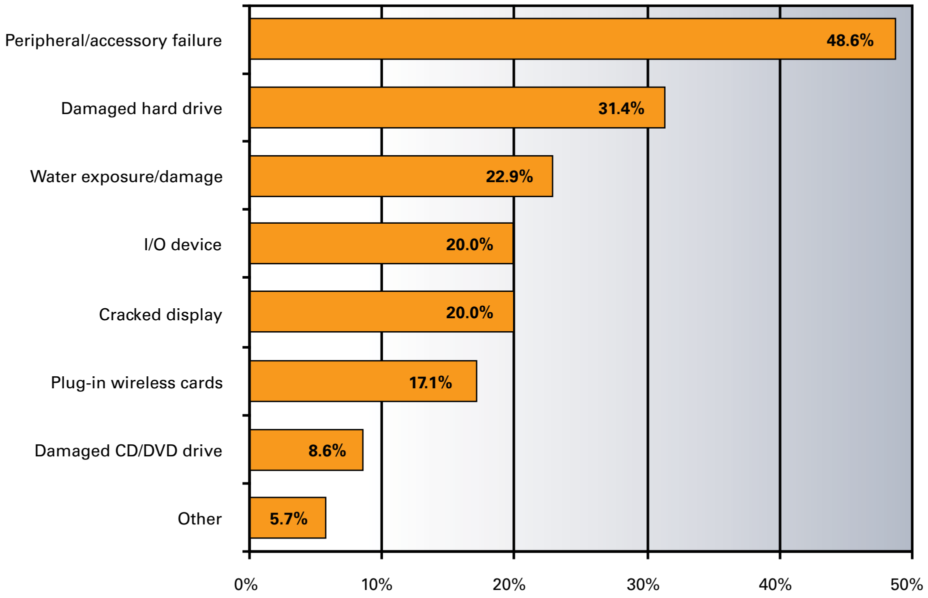
By contrast, fully-rugged devices usually offer wide-area radios built-in. This has several benefits:

- Better engineering, with designers able to integrate larger antennas into the body of the computer, or even provide external leads to connect to vehicle-mounted antennas. This results in superior radio performance and higher reliability in areas of interference or spotty coverage.
- Protection of communications module from damage. Modules installed inside a rugged computer are at significantly lower risk of breakage than exposed add-on cards that were designed for office use.

Sensitivity Training

When it comes right down to it, high failure rates on "low-cost" computers are hardly surprising. After all, a mobile computer is a collection of very sensitive, precision-engineered parts: the screen is a paper-thin glass sandwich; the CPU performs billions of operations per second on a sub-atomic level; the hard drive consists of thin metal platters spinning at 5400 rpm, separated from other parts by distances many times smaller than a human hair.

Primary sources of mobile computer hardware failure in government applications[4]
(Percent of Respondents)

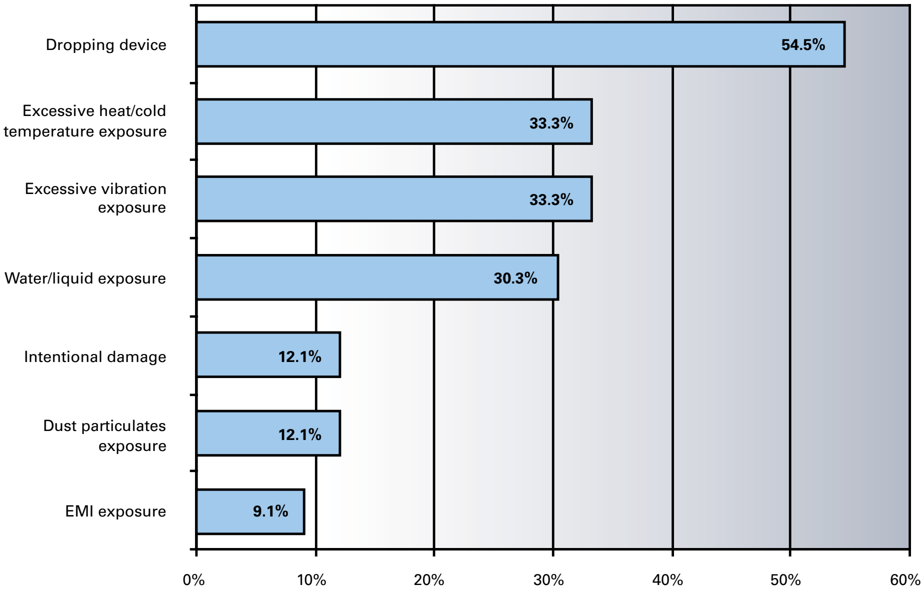


[3] "Government Mobile Deployment Trends," *Total Cost of Ownership Models for Mobile Computing and Communications Platforms*, p. 92, VDC Research Group, 2007

[4] *Ibid*, p. 109

Size, weight, appearance, and price requirements of today's consumers leave very little room for "over-engineering" or safety margins, resulting in enclosures that do little more than hold these parts together. They cannot protect the sensitive parts inside from shock, vibration, or temperature extremes. Liquids and dust have no problem getting inside, creating corrosion or gumming up mechanical parts. Such a design is an acceptable trade-off for products used in comfortable, air-conditioned homes or offices; in other environments, they don't last long.

Primary causes of mobile computer failure in government applications[5]
(Percent of Respondents)



The value of ruggedized devices is that they are designed to protect the most sensitive parts from likely damage:

- Screens are made from tempered glass, so they will not shatter if the computer is dropped
- Hard drives are mounted on shock absorbers, which protect the drive from impact when a computer is hit or dropped. The shock absorbers also dampen vibrations that can damage the drive or dislodge assembled parts.
- Cases are made from impact-resistant materials. Joints are made waterproof by design or sealed with gaskets, preventing liquids and dust from getting inside. Ports and connectors are covered.
- Optional built-in features—such as built-in bar code scanners and WAN communication modules—make fragile peripherals unnecessary.
- Stringent testing is done throughout the design, manufacture, and life of the product to make sure it meets specifications. Well-known standards are followed—for example, the U.S. military's MIL-STD-810F.

[5] "Government Mobile Deployment Trends," *Total Cost of Ownership Models for Mobile Computing and Communications Platforms*, p. 110, VDC Research Group, 2007

Conclusion

When it comes to mobile computers, government organizations should remember the old adage: *We are too poor to afford cheap things*. Devices designed and built for consumers and office workers will not stand up to everyday use in the hostile outdoor environments in which government and public safety personnel work. The extra costs of support and lost productivity from failed devices exceed any up-front cost savings within a year of two of purchase.

Government workers outside the four walls require ruggedized devices. Appropriate hardware will not only reduce TCO—it will raise productivity and increase job satisfaction.

With a decades-long legacy of leadership in providing advanced communications and computing technology to government customers, Motorola is the logical partner for government organizations looking into mobile computing solutions. With a portfolio that includes rugged handheld, notebook, and vehicle-mounted workstations, private and public data network expertise, and world-class software partners, it's no wonder government and public safety agencies turn to Motorola.

Mobile computers from Motorola are designed and tested to meet or exceed multiple ruggedness standards to serve a variety of customer needs—standards like MIL-STD-810F, IEC Ingress Protection (IP), and Motorola's proprietary 12M. Motorola computers offer support for image capture, bar-code scanning, GPS support, mag-stripe reading, signature capture, and fingerprint identification. Data connectivity options include secure connections over public wireless broadband, private data networks, as well as WiFi and Bluetooth®.

For more information, contact your Motorola representative,
or see motorola.com/mobilecomputers.

MOTOROLA

Motorola, Inc.
1301 E. Algonquin Road
Schaumburg, Illinois 60196 U.S.A.
www.motorola.com/mobilecomputers
1-800-367-2346

The information presented herein is to the best of our knowledge true and accurate. No warranty or guarantee expressed or implied is made regarding the capacity, performance or suitability of any product.