ALL YOU NEED TO KNOW ABOUT WINDOWS EMBEDDED HANDHELD 6.5 END OF LIFE.

CYBERSECURITY FRONT AND CENTER.

Cyberattacks don't seem to follow any particular pattern – everyone knows the danger is there and it's real, but it's impossible to predict when hackers might act. Fortunately, at least in the business world, this is only partly true. Cyberattacks can sometimes be anticipated. Such is the case with the Windows Embedded Handheld 6.5 End of Life.

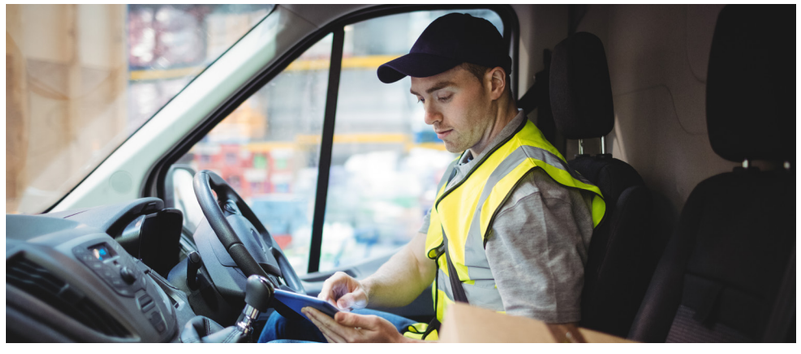
For businesses that want to stay safe, preventive measures are the best way to go. It's more important than ever for businesses to find strategies to minimize the risks of cybersecurity attacks. Hackers have the power to mar brand reputation, cause loss of business and more. A recent example is Yahoo – their huge security breaches in 2013 and 2014 affected more than 3 billion accounts and may have cost them more than $50 million in damages.[1]

The global average cost of a data breach in 2018 was up 6.4 percent over the previous year to $3.86 million, according to IBM.[2]

Numbers for 2019 have not been disclosed yet, but there are indications that they will greatly surpass last year. Juniper Research data suggests that the average cost of a data breach in 2020 will exceed $150 million.[3]

To counter future attacks and avoid rising costs of data breaches, businesses should create a culture where security is part of everything they do – from clear processes and protocols to frequent trainings. Companies storing and using sensitive data must continually assess weaknesses, current strategies, and human error potential.

When it comes to data breaches targeting the transportation and logistics sector, for instance, the most obvious consequences would be the loss of products, cargo and freight disruption to on-time delivery commitments, and having to deal with a steep decline in customer confidence.



[1]https://www.cnet.com/news/yahoo-must-pay-50m-in-damages-for-security-breach/
[2]https://www.ibm.com/security/data-breach
[3]https://www.cybintsolutions.com/cyber-security-facts-stats/

SAY GOODBYE TO WINDOWS EMBEDDED HANDHELD 6.5.

On January 14, 2020, Microsoft stopped supporting Windows Embedded Handheld 6.5. That means your devices running these operating systems will not be protected against security threats after this date.

15 million

Up to 15 million devices running on these mobile OS platforms will no longer be able to receive updates or security fixes, putting them at risk for upcoming vulnerabilities.[4]

After the Windows Embedded Handheld 6.5 End of Life date you'll still be able to use the OS, but you'll do it at your own risk. Without security updates, your data and system will be extremely vulnerable to viruses and malware. For example, if you have Windows Embedded Handheld 6.5 installed on your hand-held devices and the software gets infected with a virus, this can lead to a decrease in productivity.

Recent data suggests that any vulnerability should be treated with the utmost attention. Both the frequency and severity of data breaches are on the rise. One of the most recent examples is Uber's massive 2016 data breach that compromised over 57 million riders and drivers.[5] The individual cost for these breaches is staggering. The average monetary cost of a malware attack per company is $2.4 million but some estimates for U.S. companies reach $4.13 million.

Security and cost are no longer the only concerns. Enterprises need also to be mindful about losing functionality when these older devices will be replaced. When manufacturers stop making components for old hardware, repairs will become increasingly difficult, diminishing the usability of those devices.

Additionally, compatibility will become more challenging. Adding new devices and software ad-hoc complicates your technology environment unnecessarily if each must be made compatible with platforms that are no longer supported.

[4]https://www.rfgen.com/blog/migrate-before-its-too-late-windows-embedded-os-reaching-end-of-life/
[5]https://www.varonis.com/blog/cybersecurity-statistics/

EVALUATE YOUR OPTIONS.

Before making the decision to move away from Windows Embedded Handheld 6.5, it's important to evaluate all different scenarios.

The clock has been ticking ever since 2015, when Microsoft first announced it would be phasing out support for its mobile operating system, Windows Embedded Handheld 6.5.

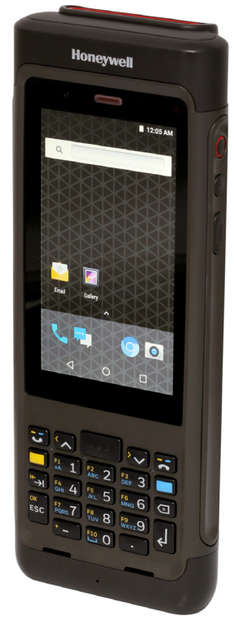
With Windows no longer a viable option for many enterprises, Android has emerged as the top contender for an operating system compatible with rugged environments. According to a VDC Research report, Android OS shares grew from 24% to 37% for all rugged handheld devices from 2015 to 2016, while Windows Embedded Handheld 6.5X/Windows Mobile fell from 49% to 39% during that time.[6]

Choosing the right mobile devices is a critical business decision. The key to making it simple for IT teams is finding devices that use a consistent deployment scheme and maintain a steady security update cadence.

No matter their size, if companies are not proactive in transitioning and their devices fail, they could put workers in a difficult place.

Users who continue to run Windows Embedded Handheld 6.5 after End of Life could be targeted by hackers. It's not uncommon for hackers to find ways to exploit vulnerable systems and wreak havoc.

While it's a good idea to have an alternative that provides security updates for your Windows Embedded Handheld 6.5 systems, migrating your devices to another operating system as soon as possible can prove to be a lower-cost solution in the long run.



[6]https://www.vdcresearch.com/News-events/emob-blog/Enterprise-Users-Brace-for-Windows-10-Leap.html

Honeywell

AB&R®
identify. track. manage.

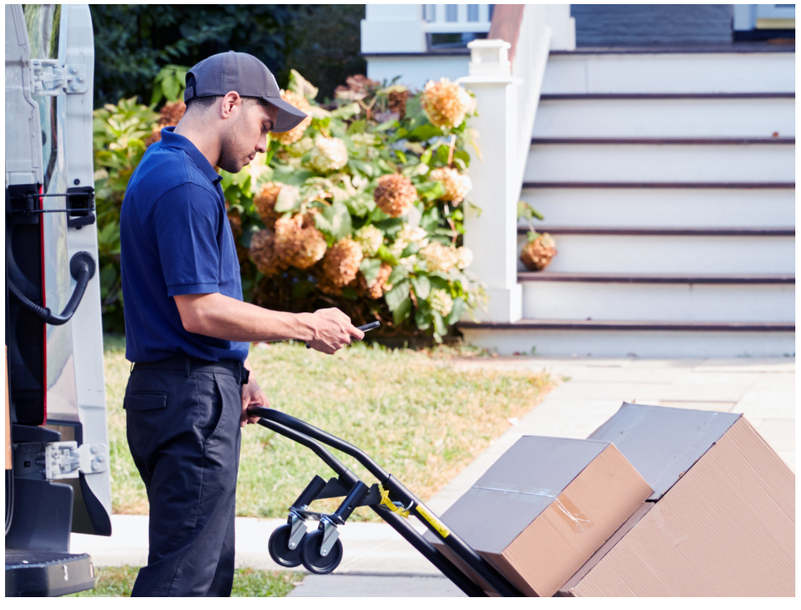
TACKLE TRANSITION LIKE A PRO.

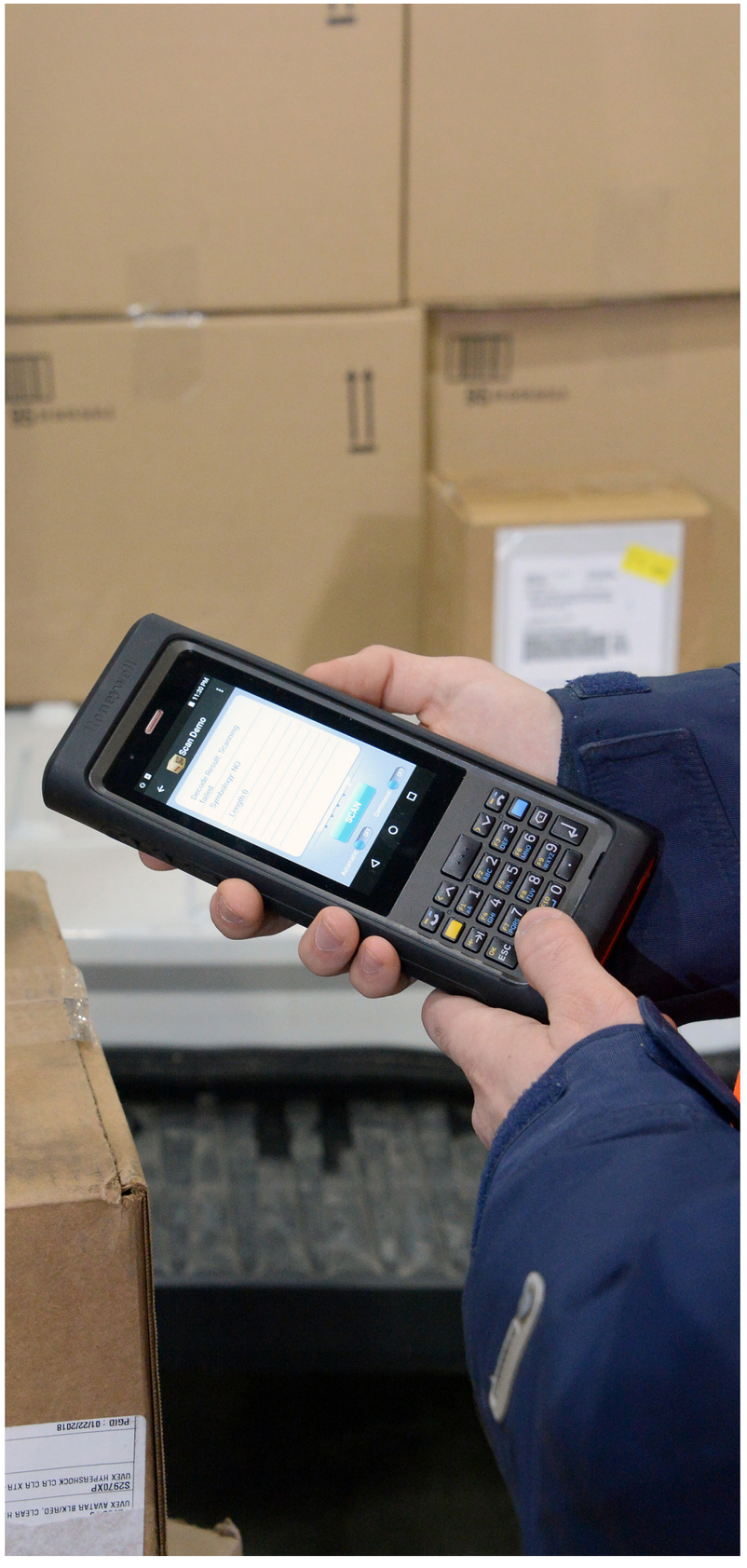
If, after evaluating all of your options, you've reached the conclusion that it's time to move on from Windows Embedded Handheld 6.5, you should start preparing for the transition right away.

There are some measures you can take to ensure minimal disruption when transitioning to a new operating system.

When migrating from Windows Embedded Handheld 6.5 you should:

- Identify all machines that need to be upgraded or replaced
- Identify and consider replacing legacy systems using older operating systems and/or software with updated technology
- Develop a timeline and budget for upgrades and replacements
- Implement security controls to separate critical systems from Windows Embedded Handheld 6.5 machines that cannot be upgraded or removed
- Plan for employee training to learn the new system





CHOOSE THE RIGHT BUSINESS PARTNER.

Replacing your old operating system may seem like a daunting task. But you don't need to make this transition by yourself. Choosing a partner with deep security expertise can help you get things up and running in no time.

Honeywell has a deep institutional and cultural focus on security across multiple domains. We invest in excess of $50 million annually in cybersecurity and employ 300+ dedicated security professionals who are focused on protecting our customers.

Honeywell's products are secure by design, informed by intelligence, and defended with vigilance so you can feel confident that applications, network, data storage and operating systems are protected.

Honeywell mobile devices also are designed to facilitate a seamless transition from Windows Embedded Handheld 6.5 to Android OS. And you can easily deploy security patches across all devices on the unified Mobility Edge™ platform – built to handle all updates through Android R. When Google ends its security patch support, Honeywell is committed to extending security patch availability for five more years via Honeywell Sentinel™, until 2028.

60 days

Honeywell provides a regular security patch cadence for Mobility Edge™ devices — at least every 90 days and often as frequently as 60 days. This way, you can rest assured that you're using the most recent version of the operating system and are up to date with all security patches.

Customers all over the world have taken their business to the next level through a partnership with AB&R and Honeywell.

LOOK TO THE FUTURE

Now is the time to make your distribution center safer, more efficient and more profitable. To achieve the best results, you need to partner with the best. AB&R has more than 40 years of experience with Automated Identification and Data Capture (AIDC) services and is a Platinum Performance Partner with Honeywell.
Our innovative Honeywell solutions meet the constantly evolving, ever-changing and always increasing demands of DC operations and deliver results you can count on—every day.

Contact AB&R® Today
info@abr.com
www.abr.com/safety-is-everything

For more information
AB&R® (American Barcode and RFID)

3431 East Elwood Street
Phoenix, AZ 85040
800.281.3056
www.abr.com

Honeywell

AB&R®
identify. track. manage.