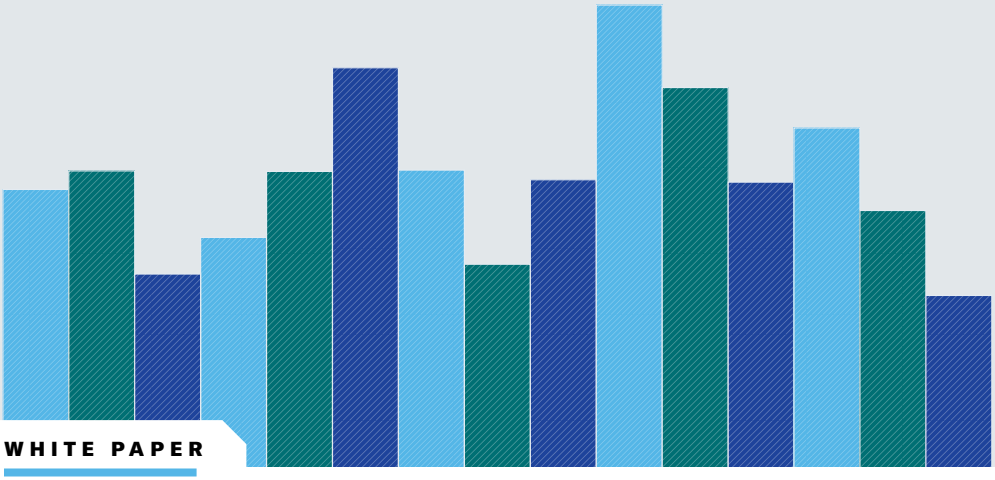
Harvard Business Review
ANALYTIC SERVICES



WHITE PAPER

The Strategic Importance of a PC Refresh

Sponsored by

intel

SPONSOR PERSPECTIVE

The hybrid work era has allowed companies to work cohesively from anywhere, but concerns around security, productivity, and the employee experience have emerged. And as the modern office continues to evolve, the technology that employers provide must adapt to meet these new challenges.

Security has never been more important. With increasingly sophisticated cyber attacks and employees working outside the firewall, older devices leave your employees vulnerable. Nearly 90%[1] of security decision makers say that outdated hardware leaves organizations more exposed, and that modern computers, on the other hand, can keep pace with modern cyber attacks and future threats. In addition, cost-effectiveness is on your side. The average security breach costs $8.19 million,[2] which far exceeds the up-front expense of an organizational PC refresh.

A fresh fleet of devices also inspires greater productivity. When employees experience tech issues, disruptions can lead to interrupted workflows and lower productivity. Computers with longer-lasting batteries and powerful processors can help empower a productive work experience with positive outcomes. Up-to-date and high-performing tools are great for company morale, which helps attract and retain top talent, ultimately leading to better performance, improved collaboration, and higher cost-effectiveness in the long run.

Intel believes updating technology allows workers to do their best work and businesses to excel. And at a time when people can work from anywhere, good technology has the capacity to transform our lives. We are sponsoring this report because we believe that a PC refresh leads to a lot of positive results, which can translate to better ROI. You'll read about the case for regular device upgrades from some of our partners, including Accenture, CDW, Lenovo, Microsoft, and ServiceNow—and how these refreshes are essential to any successful company.

We are approaching an important moment in the era of the hybrid office, and I encourage you to use this report to make the case for PC refresh. With pressing security and employee experience concerns, the time for an update is now. There's an initial investment, but a new fleet of devices can help lead to improved productivity, millions of dollars saved from potential security breaches, and the retention of your top performers to propel your company forward. Join the conversation and read on to discover the power of newer tech in the modern office.

Stephanie Hallford

Vice President and General Manager, Commercial Client Division

Intel Corp.

1 Windows 11 Security Book: Powerful security from chip to cloud, September 2022

2 Forrester, "How PCs Will Drive the Future of Work," January 2020

The Strategic Importance of a PC Refresh

As the ways people work continue to evolve, so does what they need from the personal computers (PCs), mobile phones, and other devices their employers provide. The rise of remote and hybrid work during the Covid-19 pandemic meant many employees started doing their jobs from home, which brought up very real concerns and challenges regarding security, productivity, and employee experience. Updating company technology with a PC refresh can help companies respond to all of these areas.

For the first time, the majority of many companies' workforces aren't behind a corporate firewall, the network security system, which increases the risk that employees—and companies—face from cyber threats. The greater risk is partly due to computers not having security protections that are sufficiently robust or up to date for dealing with malware and viruses that are constantly evolving. Partly it's due to hackers stepping up their attacks, such as phishing attempts on individual employees. And partly it's due to the sheer scale of IT teams having to support thousands of employees in a variety of working environments. Taken together, the scope of the task that hybrid cybersecurity presents is clear. "If you ask my large enterprise customers about their top challenges during and after the pandemic, they'd probably tell you that security is number one, two, and three," says Jerry Paradise, vice president, commercial portfolio and product management, at American-Chinese PC maker Lenovo, the world's largest by unit sales.

Security risks are also heightened because cybercriminals are increasingly sophisticated, so it's harder for people to tell whether emails, links, and attachments are trustworthy. In a 2021 survey of more than 10,000 adults in 10

HIGHLIGHTS

Security requires employees' devices to **protect them from current and emerging cyber threats**, whether they are behind or outside the corporate firewall.

When a company sufficiently invests in great tools, it can **gain a reputation as an employer that equips people** to do their best work.

As companies continue to think about their hybrid workplace technology plans, **a personal computer refresh can be a strategic initiative** that accelerates and supports multiple business goals.

"It used to be that you came into an office and 'work' was a place. Now work has turned into an outcome," says Carlos Henriquez, vice president, product and partner management–endpoint solutions at CDW.

countries by Norton, the Tempe, Ariz.–based digital security software provider, 74% of respondents said remote work has made it easier for hackers to take advantage of people, and 62% said it is difficult to determine whether information they see online is from a credible source.[1] That means hackers are at an advantage when trying to trick someone into giving them access to company systems.

Productivity and employee experience (EX) are key parts of the PC refresh equation, too. Employee devices have to help people get their jobs done without getting in their way. IT teams thus need to balance securing devices—company-issued ones and, in some cases, personal ones as well—with supporting people in doing their best work. The devices that employees use every day are a significant factor in their experience at work, so there's a retention and recruiting angle to having updated technology as well. Younger people in particular may be less attracted to a company that doesn't offer them the tools they want and need.

What all this means is that IT decision makers and senior executives alike have to take a broader, more holistic view of what a PC refresh can accomplish than they have in the past. Doing so is only becoming more important, since hybrid work is here to stay. In a 2021 survey of more than 9,000 employees from various countries and industries by Accenture, the Dublin-based consulting firm, 83% of respondents said hybrid was the optimal working model.[2] Early in the pandemic, with the overnight shift to working from anywhere, executives may not have had time to think about their long-term technology plans, or they may have invested in short-term solutions that wouldn't be sufficient in the future. Now is the time to carefully rethink how companies' tech investments are setting them up for success in this new hybrid environment, especially when planning for ambitious goals for digital transformation and advanced technologies like artificial intelligence.

Many executives today understand just how important it is to refresh their PC fleets—and that the payoff of getting it right is equipping the workforce for the business challenges that lie ahead. This report explores the importance and urgency of a PC refresh as companies plan for the post-pandemic future of work. It covers how updating employee technology helps with security, productivity, and employee experience; how IT decision makers think about the timing of a refresh; the business benefits of an upgrade; how IT executives can make the case for a refresh and address ROI; how to think through what kinds of devices support business goals; and common challenges during a refresh.

"If you think about what's going to enable your success as a business, it's going to come down to whether your most talented people can show those talents in a way that helps you meet business needs," says Aaron Woodman, vice president of Windows marketing at Redmond, Wash.–based technology company Microsoft. "And their single biggest dependency in doing their jobs is the device sitting directly in front of them."

Hybrid Work, Productivity, and Security

When it comes to how up-to-date technology benefits employees in ways older technology can't, productivity and security go hand in hand, as both depend on the processing power and capabilities that newer devices offer. Hybrid workers need to be able to do their jobs effectively and safely from anywhere, after all. Productivity requires devices to support them in getting work done rather than impeding it by breaking down or operating slowly. Security requires employees' devices to protect them from current and emerging cyber threats, whether they are behind or outside the corporate firewall. In both cases, new computers offer options that outdated ones lack.

According to Carlos Henriquez, vice president, product and partner management–endpoint solutions at Illinois–based IT solutions provider CDW, the new demands of hybrid work are a result of the pandemic, since the crisis changed the nature of what a job is. "It used to be that you came into an office and 'work' was a place," he says. "Now work has turned into an outcome." Accordingly, executives are thinking about which technology solutions can best support employees in achieving their job-specific outcomes, as well as which are most adaptable to the range of environments people will be in. For example, an employee's work setup may need to help them stay productive—and guard against threats—at home, in a coffee shop, and on the road.

To some extent, the practical side of productivity via newer devices is apparent. Computers with more efficient batteries and more powerful processers, for instance, offer employees a faster, smoother working experience. What may be less obvious is that the difficulties employees have always

faced with malfunctioning computers are magnified in the hybrid environment. Before the pandemic, an employee whose computer broke down could take the machine to the IT department for help and borrow a loaner laptop until the problem was solved. Someone who works from home, however, has fewer options. They might be able to get assistance online or over the phone, and maybe IT can mail them a loaner machine, but in the meantime, the employee may be essentially unable to do their job.

Collaboration is another key aspect of productivity, especially since remote collaboration has become the new normal for so many people. Here, too, the practical aspects of devices matter; running virtual meetings takes a lot of processing power, and often employees are using multiple apps at once. Add the extra requirements of security and working remotely, and having more-powerful computers becomes even more important. At the start of the pandemic, according to Microsoft's Woodman, when companies shifted to remote work almost overnight, many people found themselves working on laptops that couldn't handle the demands of streaming video and audio. "A lot of the devices that went home with people or were pushed into that environment weren't really built with those workloads in mind," he says. Even now, he adds, after several years of remote work, many employees may still be using machines with specifications that don't meet the minimum requirements of videoconferencing tools.

This problem is significant, of course, because hybrid work depends on good collaboration between coworkers, whether they're across town or around the world. If people can't work together easily, productivity will suffer. And the problem gets even worse for employees who start their jobs remotely, since collaboration tools may be the main way they build rapport with coworkers and managers they rarely, or never, see in person. For these workers, an underpowered computer may prevent them from feeling they're part of the team or the company.

Cybersecurity, too, has changed in hybrid work. New threats are always around the corner, which means IT teams and security officers are always staying vigilant for the best ways to protect employees.

To do that, though, they need to be able to roll out security patches and updates no matter where employees are. Before the crisis, says Michael Przytula, managing director, intelligent and digital workplaces at Accenture, IT teams could usually assume that everyone would be working on the corporate network, which made the task of securing their devices easier. Now keeping people and their computers safe on the open internet is far more complex. "It's definitely become more of a concern both from a security perspective and also from a management perspective," he says.

One major way that newer computers help is with their greater processing power, which lets them run newer, better

"By and large, people are kind of their own IT staff at home. So you have to plan for the worst. And it's always been the case that sometimes we're our own worst enemy when it comes to security and phishing attacks," says Jerry Paradise, vice president, commercial portfolio and product management at Lenovo.

software that can mount a stronger defense against attacks. And as more security software is loaded onto a device, the device needs more overhead to run it all.

Another way is by addressing known security vulnerabilities. Newer computers have security features in their hardware and software that protect against attacks that older devices would struggle more with. In addition, up-to-date devices often have their more-robust security features turned on by default, which isn't always the case with older computers. Those features are increasingly important because cyber attacks keep growing more sophisticated—and older PCs simply can't keep up with them. New ones, though, can scan for threats in the background while employees work, keeping both security and productivity high.

That kind of security configuration provides extra protection for employees—and companies can't be too careful when protecting hybrid employees away from the office. In these new modes of working, anything companies can do to make security simpler for people is a good idea. "By and large, people are kind of their own IT staff at home," says Lenovo's Paradise. "So you have to plan for the worst. And it's always been the case that sometimes we're our own worst enemy when it comes to security and phishing attacks."

New Technology, Better Employee Experience

Another key aspect of the holistic benefits of newer devices is an improved employee experience. While most companies have long invested to improve their customer experience, fewer were prioritizing EX the same way before the pandemic. Once the crisis hit—leading people to reevaluate the role that

Technology is a big part of employee experience because having new, up-to-date devices helps people be excited about their work.

work plays in their lives and to become more willing to leave employers that don't fit with their goals—executives realized that creating a great experience for employees is now table stakes for attracting and retaining talent.

Technology is a big part of EX because having new, up-to-date devices helps people be excited about their work. For knowledge workers, the company-issued devices they use every day are their physical points of connection to their jobs. Computers, mobile phones, and other devices are the tools they use to get things done, so the quality of the technology connects to their professional pride. "If people have the latest and greatest devices, it just helps them be happy," says Sankha Nagchoudhury, senior vice president of digital technology operations at Santa Clara, Calif.–based cloud software provider ServiceNow. "The pride of getting new technology puts a smile on their faces."

EX is also related to productivity and security, since employees have a much better experience at work when their tools help them accomplish their tasks instead of getting in their way or failing to protect them from cyber threats. If someone has a computer that takes 15 minutes to boot up or often freezes and has to be restarted, the employee—and the company—are losing valuable time on the job every day. And if the organization doesn't provide a better device, the employee isn't going to feel as though their experience matters to decision makers. "They're going to feel frustrated and not supported because they're not being heard about what's happening with their machine," says Accenture's Przytula.

These kinds of concerns are only growing more important with hybrid work, since employees' being out of the office creates greater distance between them, their managers, and senior executives. When technology problems come up, solving them remotely may be more difficult, and there's more risk that employees won't feel their challenges are seen or understood. That's why decision makers must carefully consider what kind of EX their company's devices are creating and be careful not to let issues become out of sight, out of mind.

When a company sufficiently invests in great tools, it can gain a reputation as an employer that equips people to do their best work. In other words, having newer technology can help with attracting and retaining talent. That's especially true for younger workers, who likely have little interest in working for a company that provides them with outdated technology. But it's equally true for workers of all ages, since everyone wants to have the tools and technology they need to thrive. If company-issued devices aren't meeting their needs, especially in the new hybrid environment, employees will wonder why—and the company's reputation can suffer. "What we're seeing is that employee satisfaction is tightly coupled with the quality of the device that they have," says Woodman.

Because of the connection between technology, recruiting, and retention, IT decision makers may benefit from partnering with HR and other EX-related functions as they think through technology strategy. While IT has the most expertise in the specifics of devices, HR teams may be able to offer useful insights into what employees need now and how their needs may shift in the future as jobs and modes of working continue to evolve. "I think you will increasingly see the support of technology be not just part of the recruiting process but the retention environment, too," says Woodman. "And that brings a business decision maker from HR into the equation."

The Timing of a Refresh

To do a wide-ranging, holistic assessment of a company's current technology, IT decision makers should consider how well devices are meeting the needs of employees and of the organization. Getting this kind of understanding can help decision makers both plan the timing of an upgrade and think through how a refresh can support business goals.

Many organizations are on three-to-four-year refresh cycles for PCs and other technology, so it may not always be the case that employees' computers are woefully out of date. However, the pandemic showed how quickly the business environment can change when equipping people to work from home became an instant necessity. Some machines may satisfy employees' current needs, but IT executives should continually keep an eye on the state of their PC fleets and which devices may need to be replaced sooner rather than later. If employees shift roles or take on new responsibilities, for example, they might require lighter machines that can be carried around more easily, more-powerful ones with extra memory and storage, or even new devices, such as extra monitors for their home workspaces.

And while IT decision makers may have a solid grasp of the company's strategic goals and what matters to different functions, they should stay on top of shifting priorities and how employee devices factor in. Doing so will continue to be essential as hybrid work evolves and new modes of

working—and new needs and challenges around them—emerge in the future.

In addition, IT decision makers should consider how a refresh can support other business goals that rely on having updated devices, like undergoing a digital transformation or laying the groundwork for tools like artificial intelligence and advanced analytics. Coordinating an upgrade with these kinds of efforts can help ensure their success; putting it off may make the effort far more difficult.

Frank Ford, head of the global cybersecurity practice at Boston-based consulting firm Bain & Co., says an overarching concern with the timing of an upgrade is that technology is always advancing. Even if employees' devices work well right now, new software and new tools are always being released, and people will need faster PCs to run them. "You really do need to keep your tech on pace with the tools that your employees are using," he says. Beyond that, sooner or later the devices' manufacturers will stop making spare parts needed for repairs and will stop supplying updates to operating systems, software applications, and security patches. When those updates cease, maintaining productivity and security gets harder. "Once you hit that point, it's very difficult to secure the workstation if there are new vulnerabilities that become exposed or that people become aware of," he explains.

At the same time, in some cases IT executives may have reasons to delay a refresh. One common reason, unsurprisingly, is cost. Przytula says that because buying thousands, or even tens of thousands, of new machines is a huge expense, senior executives may view an upgrade as easy to cut when they're looking to save money. "Organizations may have a stated goal around updating devices, but it always seems to be one of the first things that gets pushed back when budgets get tight," he explains.

The downside of saving money now, he continues, is the ripple effects that will continue over the next few years. If an organization lets a refresh fall by the wayside, it won't be long before employees are stuck with machines that are five or six years old. Such a situation could have serious implications for productivity, security, and EX—not to mention customer experience, since employees who can't do their jobs well will struggle to serve customers well. So before putting off the upgrade, decision makers should think through how the delay will affect current employees as well as prospective ones who may have a negative view of being given older technology when they're hired.

Security is also a key element in the timing of a refresh, especially when employees' devices are starting to age. There are no simple answers when assessing how new a device should be for optimal security; the only certainty is that, in general, newer devices protect people better than older ones do. Decision makers should be careful to balance factors like budget against the risks and potential costs that come with letting employees use machines with weaker security capabilities. According to the Hamburg-based statistics database Statista, the average cost of a data breach in the United States in 2022 was $9.44 million.[3] Przytula says this new remote element of security has to be a core part of cybersecurity plans. "It's becoming a new benchmark that companies are thinking about," he explains. "Looking at the devices you have in the field, are they remotely supportable? Are they remotely securable?" If not, updating them could be a good idea.

"You don't really have the choice to not upgrade technology. It's more a question of frequency," says Frank Ford, head of the global cybersecurity practice at Bain & Co.

Bain's Ford adds that sometimes organizations do need to keep older machines around, perhaps because they're running applications or systems the manufacturer hasn't updated or because they're too costly or complex to replace. In these cases, it's important to assess the security risks the devices could present—because many firms already struggle with everyday cybersecurity. "The reality is that most companies have a real challenge in following even basic best practices related to security," he says, especially when establishing standards across regions or countries. The challenge is more complicated than ever, he continues, since many business tasks today involve people accessing or analyzing data from various sources as well as using cloud-based software and data sources, which can open up new avenues for an attack. The thing to remember, Ford explains, is that eventually a refresh does need to happen. "You don't really have the choice to not upgrade technology," he says. "It's more a question of frequency."

The Business Case for an Upgrade

Given the range of goals that a refresh can support, how well do decision makers understand the benefits when considering it? On one hand, says ServiceNow's Nagchoudhury, most senior executives today accept the importance of upgrading technology on a regular basis, which may make the decision simpler. "Even a couple of years ago, most IT people had to

"It requires IT pros to expand their lens to understand the totality of the problem that a refresh can help with but also to expand their vocabulary to translate it into the broader organizational mission," says Aaron Woodman, vice president of Windows marketing at Microsoft.

justify the refresh," he says. "Now digital is part of business, and the conversation has become much easier."

On the other hand, according to Woodman, different companies and industries don't always think about a refresh in consistent ways, which prevents them from getting a broad enough perspective on its benefits. A better approach, he says, would be for decision makers to embrace a wide view of what upgrading devices can accomplish. "It requires IT pros to expand their lens to understand the totality of the problem that a refresh can help with," he says, "but also to expand their vocabulary to translate it into the broader organizational mission." Doing so can help IT teams and senior executives alike see a refresh as a strategic priority for the company.

When IT decision makers do have to make the case for a refresh, focusing on the connections between all its factors can help. For example, outlining the improvements to security is a good start, and security quickly brings up other relevant aspects of hybrid work, productivity, and employee satisfaction. Showing senior decision makers how these factors overlap through employee PCs emphasizes the holistic outcomes that a refresh can support.

It's worth noting, however, that measuring the return on investment of a refresh can be tricky. According to Nagchoudhury, many companies don't bother because they already grasp the initiative's importance. "To keep the lights on, they know they need to upgrade," he says. Other aspects of a refresh involve intangibles that are hard to measure. New machines can help improve employee experience, for example, but it's difficult to put a dollar amount on how much. Paradise says that a good approach to ROI is to combine total cost of ownership calculations with surveys about employees' experiences with their technology. "That will give most organizations a fairly good view of what the refresh will do for them," he says.

Ford adds that ROI measurements should be focused on the productivity benefits of an upgrade, since thinking about what new devices will help employees do can provide a more tangible metric. "It's more about the new tools and capabilities that you're putting in the hands of your people," he explains, "not so much the PCs themselves."

Devices That Meet Business Needs

Given the range of business goals that a refresh can support, the varied needs of employees and business units, and the sheer number of devices and configuration options on the market, IT decision makers may wonder what machines to buy in a refresh.

Some of the main factors to think about, according to CDW's Henriquez, are ability, reliability, manageability, and risk mitigation—that is, how well devices meet business needs, how well and for how long they'll operate, how easy they are for IT teams to support, and how robustly they provide protection against cyber threats. "You really want to provide an enhanced user experience that leads to the most productive, secure environment," he says.

To make the task easier, many companies develop employee personas, or profiles that group people based on their priorities, needs, and challenges. Organizations have long used personas to better understand their customers, and doing so for employees offers a similar benefit, especially with EX being a top priority for senior executives. Planning a refresh of personas can help ensure that new devices target the factors that will best help the workforce succeed.

There are some standard employee personas that IT teams use across companies and even industries, but it can also be helpful to customize personas to a company's employees. While the specifics of some roles may fit well with standard personas, others may require additional details, from hardware specifications to preloaded software. For example, Nagchoudhury points out that even roles within one job type can vary greatly, which affects the specifics of the devices employees need. "For a company like ours, within engineering there are more than 5,000 people, and they are not the same. They don't do the same work," he says. Someone in user experience, for example, might have very different requirements than someone in software programming. So, depending on their tasks, employees may need more- or less-powerful machines or computers with other custom specs. Nagchoudhury says that IT teams can benefit from further dividing personas into "subpersonas" when more nuance is needed.

Grouping employees this way is helpful, according to Przytula, because although IT teams may want to minimize the number of makes and models they have to support, employees like to have some choice in the devices they use. Segmenting

"Choice is one of the things that we see organizations wanting to provide while also trying to keep that pool of devices as small as they can," says Michael Przytula, managing director, intelligent and digital workplaces at Accenture.

employees by persona can help IT decision makers provide people with a few options based on the type of work they do, such as different screen sizes or different brands. "Choice is one of the things that we see organizations wanting to provide, while also trying to keep that pool of devices as small as they can," he says. When IT teams need more information about what would help employees the most, partnering with managers who are close to people's daily work or surveying employees themselves can bring new insights.

Another option for a refresh, one that is becoming more common, is to shift to a device-as-a-service model. In this approach, rather than buying thousands of new machines, the company pays a service provider to handle the organization and management of the refresh as well as ongoing support of the machines. Outsourcing the refresh this way has a few benefits. At the top of the list is the financial side of it, according to Annie Witte, assistant teaching professor of accounting at Northeastern University. A large IT infrastructure investment is treated as a capital expenditure, which means the asset will be expensed over its life as it is used. These investments often have significant cash flow implications and additional costs related to interest expense when leveraged with debt. Further, IT decision makers may have to justify the expenditure of a new refresh to financial managers before the full value of a previous refresh has been exhausted. With the device-as-a-service model, a refresh can instead become a recurring operational expense. The difference in classification affects the nature and size of how an expense may appear on financial statements. Since the fee to the service provider may be less than the depreciation expense on an annual basis, the refresh becomes a smaller income statement line item as a cost in firms' day-to-day operations. The alternative approach to a refresh may help save money over time by reducing depreciation and interest expenses and by smoothing both earnings and cash flow.

Among other benefits, the service provider can take the lead on factors like security and managing the size of the PC fleet. Having a partner ensure that devices are up to date with security patches and other precautions can help provide consistency across the firms' devices. And outsourcing devices rather than owning them outright can give companies the flexibility to scale their PC fleets up or down as their needs change. "That model has become one of the ways that we've seen clients proactively work around the challenges of a refresh," says Przytula. Executives who are looking to lower the cost of a refresh or try a new approach may want to consider the device-as-a-service model.

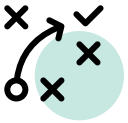
Overall, the guiding light of a PC refresh should be fairly simple, according to Woodman. This is the consideration he offers as a north star—whether your best employees have tools that help them do their best work efficiently and safely. "Can they be productive while IT manages their ability to perform in a secure way that doesn't put the organization at risk?" he asks. A refresh should be focused on offering devices that answer the question with a yes.

Challenges with a Refresh

There are several challenges that companies may run into when implementing a PC refresh, and they demonstrate the holistic nature of the initiative.

First is the logistical burden of rolling out a refresh in a hybrid environment. Swapping employees' devices was a more straightforward—if still complex—task when nearly everyone worked in the office, since the IT department and employees were in physical proximity. Now, with many people working remotely, IT teams have to navigate the added complexity of getting new machines set up, secured, and shipped to employees wherever they are. They may also run into procurement and supply chain issues when ordering new computers, a problem that was amplified by the pandemic and still affects companies today. On the back end of the process, IT teams are also dealing with how best to handle devices that aren't being used anymore, such as safely refurbishing or recycling them, once again overcoming the logistical hurdle of doing it all remotely. For now, many companies are still figuring out the optimal way to tackle these issues.

The good news for replacing old machines is that the downtime involved in moving employees to new devices can be less than it was in the past. The move has often been a headache for both IT and employees, since files, bookmarks, and other data had to be copied to the new computer, interrupting people's productivity during the workday. Now, with cloud storage in use by many companies, transferring everything has become much easier, according to Nagchoudhury. Some software may need to be reinstalled manually, but the overall hit to productivity is much lower. "People can just log in to



"The PC is the window to really deliver on transformation and anticipate those future needs, because these devices last many years. We don't see the tech requirements [of future goals] going down. They're continually going up," says Lenovo's Paradise.

their new hardware, and they should have access to pretty much everything they need," he says. For companies that haven't invested in cloud solutions yet, it's worth considering how doing so could support their PC refresh goals.

Second is the need to have a strategic plan for technology. While some companies may think a PC refresh is an end in itself, the range of areas it touches—from productivity to security to EX and beyond—shows that an upgrade initiative has the potential to support both the company's current technology goals and its future ones. For an ambitious, high-priority initiative like digital transformation, for example, employees' computers are part of the digital backbone. For that reason, technology executives need to ensure the company has a cohesive plan for which technology it's investing in and how it will enable other ambitious, high-priority initiatives later on. "The PC is the window to really deliver on transformation and anticipate those future needs, because these devices last many years," says Paradise. "We don't see the tech requirements [of future goals] going down. They're continually going up." Without a plan, companies may find themselves investing in areas that don't serve them well.

Henriquez agrees with the importance of having a technology plan, and he adds that it should take into account the range of areas that a refresh touches. He adds that tech plans are different for every company, so it's imperative that decision makers understand their company's specific business and technology context. "It's about understanding the technology, understanding the worker experience, capturing worker input, understanding all those related factors, and researching them and using them to put together a plan," he says. "But it is different for every company."

A third challenge is how much emphasis companies' vendors and other partners put on security, especially when companies are upgrading their defenses. Firms will want to make sure their partners' security is at the same level of capability as their own. Przytula says there are a few main strategies here. Some companies may mandate that anyone doing work for them must use a company-issued device, which gives the firm control over security and other concerns. Other organizations may provide a virtual desktop environment that gives access to their systems in a controlled way. And other companies may write security specifications into the vendor contract so both sides agree to keep their operating systems and security patches at certain levels. Whatever method a company uses, Przytula says it's essential to be on the same page when it comes to cybersecurity and the risks of a breach. "There's definitely some trust required in some of those scenarios," he says.

Conclusion

As companies continue to think about their hybrid workplace technology plans, a PC refresh can be a strategic initiative that accelerates and supports multiple business goals. It can improve security, bolstering an organization's defenses against cyber threats. It can empower hybrid work, giving employees the tools to do their jobs flexibly and effectively from anywhere. It can help with creating a great employee experience, which in turn helps with recruiting and retention. It can create a foundation for future ambitious technology goals. And it can even save companies money in the long term, whether through offering people newer machines that need less maintenance or by switching to a device-as-a-service approach. All of these factors show how a refresh can holistically affect many aspects of the organization.

Simply put, decision makers who put off an upgrade risk their company becoming the next big security breach headline—and putting the firm's data, customer trust, and reputation in peril. At a minimum, employees won't be equipped with the tools they need to serve customers well or to tackle the challenges that the future of work is bringing. Says Woodman, "You get employees that are essentially doing their best and giving you 75% of what's possible."

Endnotes

1 Norton, “2021 Norton Cyber Safety Insights Report: Global Results,” May 2021. https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf.

2 Christie Smith, Yaarit Silverstone, Nicholas Whittall, et al., “The Future of Work: Productive Anywhere,” Accenture, 2021. https://www.accenture.com/_acnmedia/PDF-155/Accenture-Future-Of-Work-Global-Report.pdf.

3 Statista, “Average Cost of a Data Breach in the United States from 2006 to 2022,” 2022. https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach.

Harvard Business Review
ANALYTIC SERVICES

ABOUT US

Harvard Business Review Analytic Services is an independent commercial research unit within Harvard Business Review Group, conducting research and comparative analysis on important management challenges and emerging business opportunities. Seeking to provide business intelligence and peer-group insight, each report is published based on the findings of original quantitative and/or qualitative research and analysis. Quantitative surveys are conducted with the HBR Advisory Council, HBR's global research panel, and qualitative research is conducted with senior business executives and subject matter experts from within and beyond the *Harvard Business Review* author community. Email us at hbranalyticservices@hbr.org.

hbr.org/hbr-analytic-services

MCCRE37400523