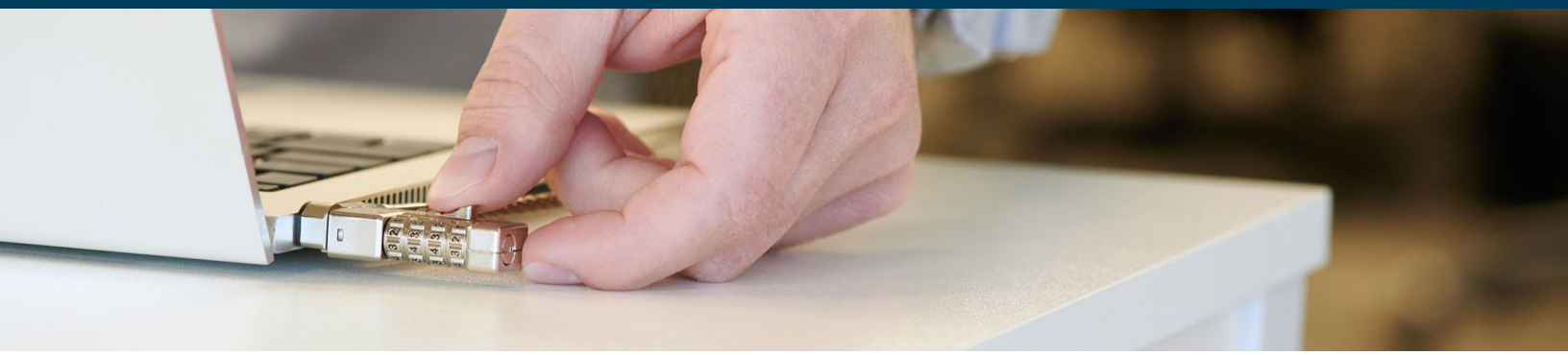
Kensington®

Secure Your Device, Protect Your Data.

How physical security can help prevent your next data breach



Introduction

The security landscape has evolved dramatically in recent years, driven by transformative shifts in how and where we work. The ultimate driver in this was the COVID-19 pandemic; it accelerated the adoption of hybrid and flexible working models and fundamentally altered device security priorities.

Kensington sponsored a study conducted by independent market research specialist Vanson Bourne, of 1,000 senior IT decision makers with responsibility for their organization's physical hardware security across the US and EMEA. Nearly all surveyed (**92%**) tightened their security policies in response to the pandemic, recognizing the heightened risks associated with decentralized work environments. As we look toward 2025, the level of more flexible working models is expected to rise, emphasizing that the time to rethink device security strategies is now.

Data breaches aren't just a digital problem—every stolen or unsecured device represents a potential gateway for unauthorized access to sensitive information, posing significant risks for organizations. With the financial burden of a data breach now averaging millions of dollars, the stakes have never been higher. As organizations continue to adapt their working models, the urgency of addressing device security has grown massively. Stricter data protection requirements and a surge in data breaches have further elevated the importance of safeguarding both physical devices and the sensitive information they hold. This report highlights the critical role security locks play in mitigating these risks and underscores why taking action now is essential to stay ahead of emerging challenges.

Through these findings, we will examine the tangible impacts of device theft, showcase how simple yet effective solutions like security locks can help to mitigate risks, and highlight how physical security provides peace of mind in a world where working models are constantly evolving. From understanding the staggering consequences of device theft to demonstrating the cost-effectiveness and reassurance of locks, this report provides actionable insights for organizations navigating today's complex security landscape.

Key findings:

76% of respondents say their organization has been impacted by incidents of theft in the last 2 years, with incidents more common in organizations with more flexible working models. For instance, our research revealed that (**85%**) of organizations with flexible working models experienced an incident of theft in the last 2 years, compared to **71%** of organizations whose employees are fully onsite.

The impacts of device theft extend beyond hardware loss, including:

- the need to enhance existing security measures (**33%**)
- legal or regulatory consequences due to compromised data on stolen devices (**33%**)
- disruption to employee productivity from lost or stolen devices (**32%**)

Organizations using security locks were **37%** less likely to experience a data breach caused by an unsecured device (**38%** vs. **60%** among those who aren't using security locks).

Organizations currently using locks were also more likely to be using a dual approach to security, with three quarters (**76%**) using digital measures like fingerprint or security keys for two-factor authentication, compared to **62%** of those not using locks at all.

84% agree security locks are cost effective in mitigating potential data breaches, offering significant value for relatively low investment.

- **42%** believe device locks to be extremely cost effective, providing high protection at low cost, with the most senior leaders more likely to recognize their value (**56%**) compared to mid-level management (**36%**).

Almost all surveyed (**98%**) believe device locks may prevent theft, reducing the likelihood of unauthorized access to sensitive company data.

Stolen Devices, Staggering Consequences

Rarely a day goes by where you don't hear about some sort of security incident – whether it's a large-scale attack on a global conglomerate, or more targeted exploit of critical infrastructure or service. And while those examples suggest that cyber incidents are often the most widely discussed – or at least assumed to be – it's important to recognize that physical security threats can be just as critical.

There's little widespread conversation about physical security incidents, where unauthorized people gain access to secured areas or compromise assets, which have just as dire consequences as the average ransomware attack. According to our research, over three quarters (**76%**) of those surveyed say their organization has been impacted by incidents of device theft in the last two years.

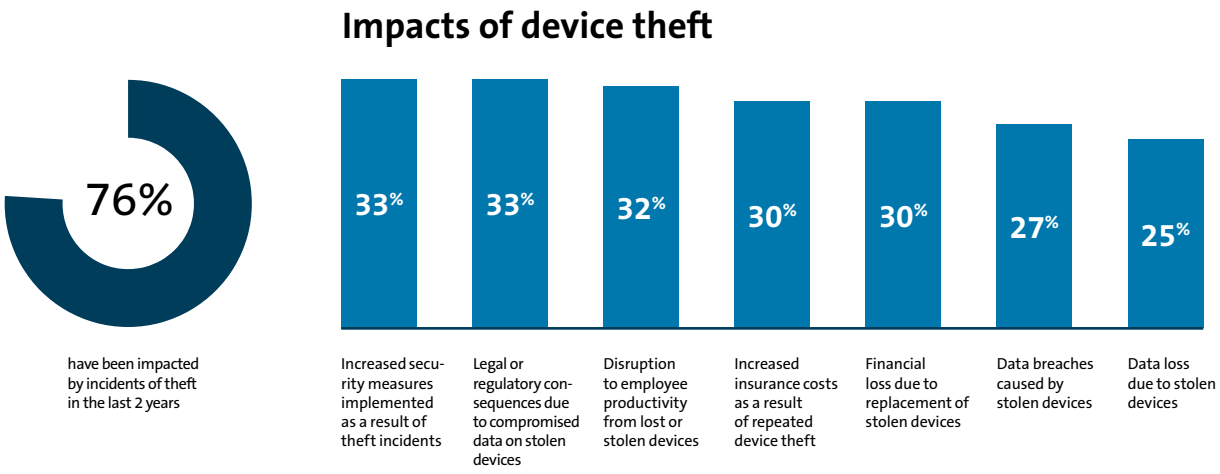


Fig. 1: *How has your organization been impacted by incidents of device theft in the past two years? [Asked to all respondents: 1000]*

It's not just the obvious cost of replacing a device that organizations are faced with (**30%**). The most common impacts include an increase in security measures implemented as a result (**33%**) or legal or regulatory consequences due to compromised data (**33%**), where the latter is often clearly outlined. For example, GDPR[1] fines can reach up to 20 million euros or **4%** of an organization's global turnover, with even less severe violations costing up to 10 million euros, posing significant financial risks for non-compliance. Adding to the financial impacts is the cost of disruption to employee productivity from lost or stolen devices (**32%**) as well. Off the back of any of these impacts, there's a clear financial or time implication on the organization's bottom line. So, it's not just digital security incidents that demand attention—physical threats pose significant risks as well. By deepening their understanding of these vulnerabilities, organizations can take simple, cost-effective steps to safeguard their devices. With physical security measures being both affordable and easy to implement (as we'll explore later), they represent a practical first step in strengthening overall security.

"In addition to cybersecurity measures, **physical security is equally important**. Secure cables are part of a stronger cybersecurity strategy."

Senior management; Manufacturing and production; 1,000 or more employees; Fully onsite working model; France

1 GDPR Fines/Penalties, Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/

In the modern day, it's not a case of if a data breach occurs, but when. In fact, every single device theft is a data breach waiting to happen, and the financial implications are staggering for organizations. According to IBM's most recent cost of data breach report[2], the global average cost of a data breach in 2024 sits at $4.88 million USD; a rise of **10%** in a year from $4.45 million USD average in 2023. This figure differs across industry and size of organization, so some organizations may face even higher.

Spotlight on the data:

- **Sector:** organizations in the consumer services (**95%**), Energy, oil/ gas and utilities (**90%**) and construction and property (**89%**) industries are the most likely to have been impacted by device theft. The higher mobility of employees and devices across these businesses exposes them to greater risk of theft
- **Size:** the likelihood of device theft in smaller organizations (100-249 employees) has increased more (**82%**) than in larger organizations with more than 1,000 employees (**69%**), highlighting the relative impact to smaller organizations where resources are more limited, the impacts may be more pronounced
- **Seniority:** Those in more senior positions are much more likely to report they've been impacted by incidents of thefts (**87%**), than mid-level managers (**67%**). It's likely those in charge of running the day-to-day of a business are ill-informed of the potential threats facing unsecure devices. Increasing their awareness of the threats, and the associated repercussions, will help encourage businesses to embed security locks into their cultural needs and align perspectives across all levels to support a comprehensive security strategy

How do working models play a part here?

We noted as we introduced this research the sheer change in ways of working over recent years, with the adoption of more flexible working models away from a fixed place of work having been accelerated by the COVID-19 pandemic.

Where we see over three quarters (**76%**) of all those surveyed reporting that their organization has been impacted by device theft in the last 2 years, this becomes more apparent where working models are more flexible – rising to over 9 in 10 (**94%**) where employees are fully remote.

Pervasiveness of device theft in the last two years, by current working model

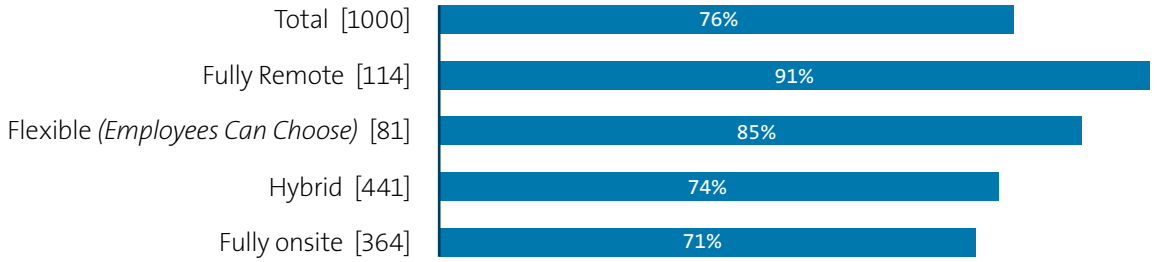


Fig. 2: *Proportion of respondents whose organization has been impacted by incidents of device theft in the past two years [Asked to all respondents, showing data split by current working model, base numbers in chart]*

2 Cost of Data Breach Report 2024, IBM, July 2024, https://www.ibm.com/reports/data-breach

While it's important for any organization to be mindful of physical device security, and wary of the impacts of device theft, flexible and remote working models significantly amplify the risk of device theft, making robust security measures more critical than ever.

It's important to note the level of device theft is generally high, even when employees are fully onsite – organizations have no room to be complacent regardless of where their employees work. The device theft threat isn't new and hasn't just appeared as part of this post-pandemic world either. Our research in 2016[3] investigated the security risks created by IT theft in the enterprise. Surveyed IT professionals ranked the risk of device theft in the office (**23%**) almost as high as theft in cars and transportation (**25%**), and more than theft in airports and hotels (**15%**) or restaurants (**12%**). This shows how device theft remains a persistent threat, even in fully onsite environments, underscoring the need for vigilance and proactive physical security measures regardless of workplace setting.

This challenge has been further amplified in the post-COVID-19 world, with **93%** of organizations reporting an increase in security risks due to the shift to flexible and hybrid working models. These risks extend beyond physical device theft to include heightened vulnerabilities in data protection, unauthorized access, and breaches caused by unsecured home networks and decentralized working environments.

"**It is the easiest way** to make sure that our devices are under literal lock and key! It makes it so that **we know everything is safe and secure**"

Board member/C-level; IT, technology and telecoms; 100-249 employees; Flexible working model; USA

Security risk increases as a result of hybrid or remote working environments

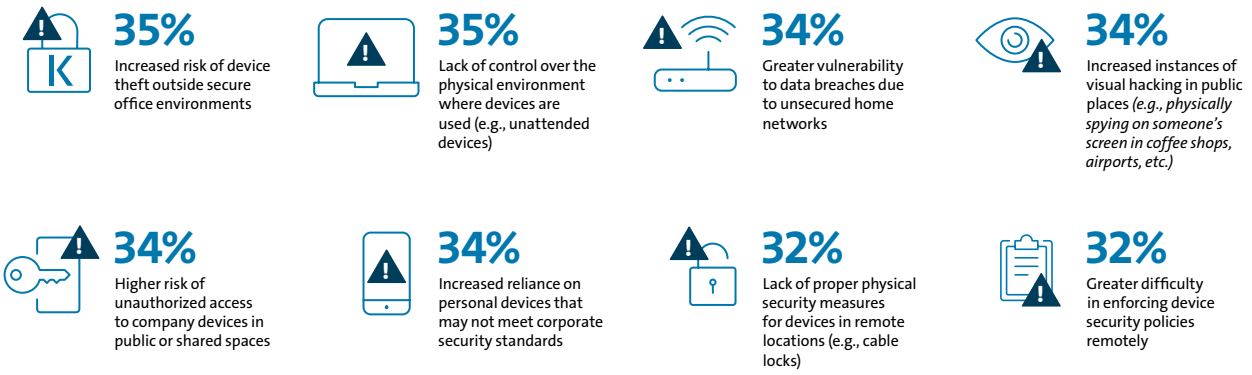


Fig. 3: *In your opinion, what security risks have increased as a result of hybrid or remote working environments following the COVID-19 pandemic? [Asked to respondents whose organization saw a shift towards hybrid/remote work following the COVID-19 pandemic: 494]*

With this in mind, the best approach to security lies in combining robust physical measures with advanced digital safeguards, ensuring comprehensive protection for both devices and data in an increasingly decentralized world.

3 IT Security & Laptop Theft Survey, Kensington, August 2016, https://www.kensington.com/news/news-press-center/2016-news--press-center/kensington-survey-data-reveals-that-it-theft-in-the-office-ranks-nearly-as-high-as-theft-in-cars-and-more-than-in-airports-or-restaurants/?srsltid=AfmBOooRTMdZ4gjmcNB3viXIJcIL4GY47XxO5I08AldLhLEB5LjnH0Ts

Locks That Stop Loss—And Save Costs

"The lack of a security lock on the equipment led to a data breach, **resulting in significant losses for the company.**"

Mid-level management; IT, technology and telecoms; 1,000 or more employees; Flexible working model; USA

So far, we've uncovered the consequences of device theft, and how pervasive this can be regardless of working environment. Yet, this isn't the only concern for our surveyed senior IT decision makers. There's a wide range of aspects they're worried about when it comes to security, across both physical and digital areas.

Some of these concerns present newer factors around physical security. For example, almost a quarter (**23%**) are concerned by visual hacking, where sensitive data is at the mercy of anyone if someone's screen is on show in a public place – in a coffee shop or on public transport. In fact, those who work flexibly (**48%**) are more likely than those in fully remote (**36%**) or hybrid (**33%**) setups to report visual hacking as a concern. This highlights that visual hacking isn't just associated with working from home, but rather with granting excessive freedoms that are more difficult to control. Organizations will need to take consideration towards protecting their data when employees are out and about, through additional deterrents like privacy screens.

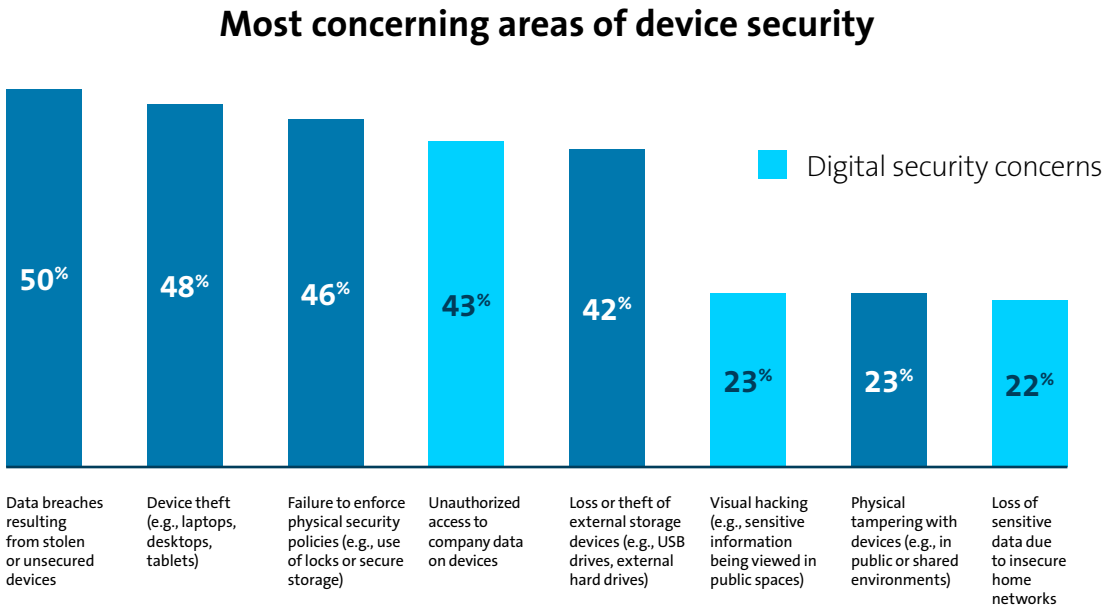


Fig. 4: *Which areas of device security in your organization concern you the most? [Asked to all respondents: 1000, showing the combination of responses ranked first, second and third]*

Data breaches are the number one concern though, which is well-founded as a notable proportion (**46%**) have experienced a data breach as a direct consequence of an unsecured device.

This is where a security lock can help. Organizations using security locks are **37%** less likely to have experienced a data breach because of an unsecured device vs. those who aren't using security locks at all.

Organizations that have experienced a data breach or loss of sensitive data because of an unsecured device

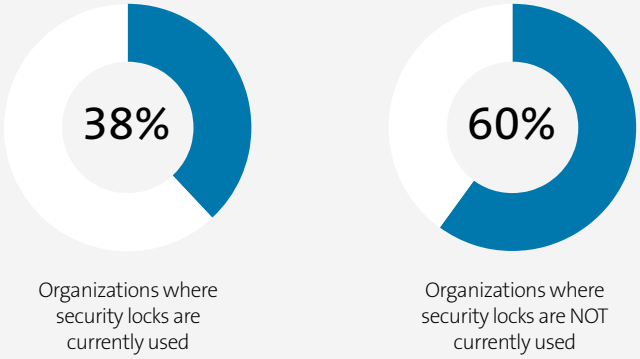


Fig. 5: *Has your organization experienced a data breach or loss of sensitive data as a direct consequence of a device being left unsecured? [Asked to all respondents, split by those currently using security locks: 629; and those not currently using security locks: 371]*

The outcome is clear: demonstrating a measurable reduction in data breaches or data loss reinforces the value of security locks as a critical component of comprehensive device protection. This compelling evidence highlights how security locks directly mitigate risk, positioning them as an essential investment for organizations committed to safeguarding their data and minimizing security vulnerabilities.

Spotlight on the data:

- **Sector:** based on survey results, organizations in the consumer services (**65%**) and public/private healthcare (**57%**) industries are more likely to have experienced a data breach as a consequence of an unsecured device. The former was among the most likely to have been impacted by device theft generally. With the latter, this perhaps highlights bigger concerns for the decentralized nature of healthcare institutions and members of the public being in closer contact with devices. Having such a wealth of sensitive data puts this sector at greater risk
- **Size:** further highlighting the limited resources of smaller organizations, they're more likely (**59%**) than their larger counterparts (**40%**) to have experienced a data breach because of an unsecured device. Not only do they struggle with the initial deterrents, but also the snowball effect that follows
- **Seniority:** the more junior of those surveyed are less likely to report a data breach or loss of sensitive data because of an unsecured device (**30%**), than their board/C-level colleagues (**59%**). There's a clear misalignment within businesses when it comes to a true understanding of physical device security and the consequences of this not being in place – a call for wider education and knowledge sharing

"A little initial investment in security measures (locks) can **considerably reduce the possibility of costly device replacements** or prolonged downtime."

Senior management; Education – government/ state provided; 1,000 or more employees; Hybrid working model; USA

So, how should organizations look to overcome this?

Organizations are faced with so many digital and physical security concerns, and the impacts of device theft are staggering for organizations and their bottom lines. They should be looking for the most cost-effective solution. And with their proven success, that could sit with the simple security lock.

The majority (**84%**) of our surveyed senior IT decision makers say security locks are cost effective in mitigating potential data breaches – that they offer significant value in preventing theft and breaches. Furthering this, **42%** believe they're extremely cost-effective.

This is a universal opinion shared by those already using security locks and even those who aren't – which does beg the question, why not? Organizations might view locks as adding logistical challenges to device management or perhaps a stronger focus on digital over physical security leads to an underestimation in the value of locks, therefore hindering adoption. Yet, when compared to the staggering financial consequences of device theft, the cost of a security lock - typically averaging as little as $30 to $50 per device - represents a minimal investment for reducing risks. Diving into this further, we see a clear difference in opinion across the organizational hierarchy.

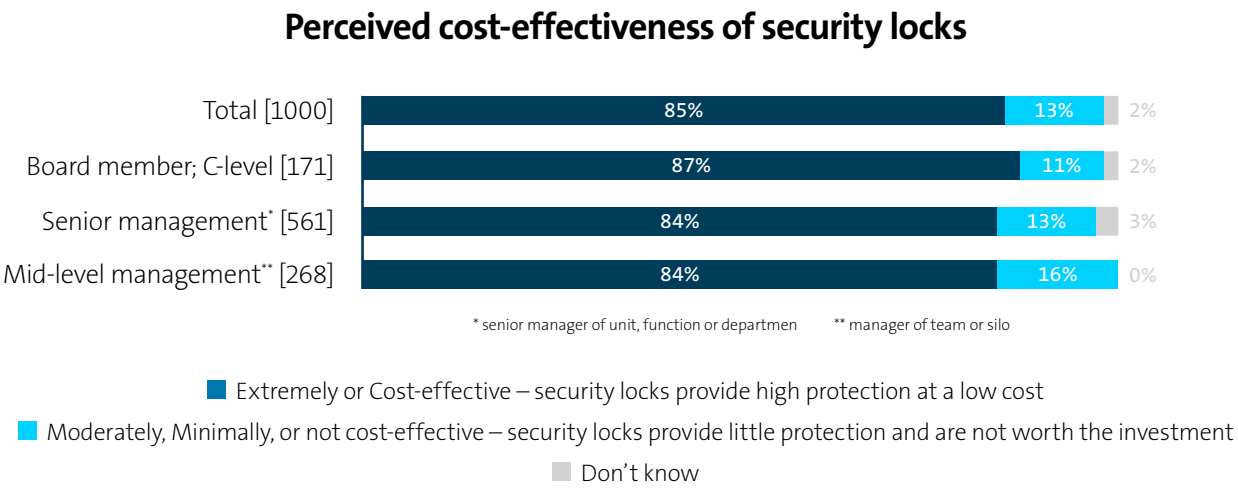


Fig. 6: *In terms of cost-effectiveness, how do you view the role of physical security locks in mitigating potential data breaches or theft? [Asked to all respondents, showing data split by seniority, base numbers in chart]*

These findings emphasize the critical need to address the root causes of device theft and its broader impacts across an organization. While senior leaders are more likely to view security locks as extremely cost-effective (**56%**), this belief diminishes at lower levels of the hierarchy. Ultimately, senior leaders will always be more focused on broader implications (e.g., regulatory fines, reputation), while lower-level managers on the day-to-day impacts (e.g., productivity loss).

This disconnect highlights the importance of organizational alignment and education around the value of security locks - not just as a cost-effective tool, but as a proactive solution to prevent significant losses before they occur. Bridging these gaps in perception will ensure a unified and effective approach to mitigating the risks of device theft and protecting sensitive data.

"Once lost, it will cause significant losses. We need to **solve this problem at its root.**"

Mid-level management; Healthcare - privately owned; 1,000 or more employees; Hybrid working model; USA

Locks Work to Secure and Reassure

We've continued to explore how security locks are not only effective in reducing theft but also offer a cost-efficient solution to mitigate broader security risks. Their diverse applications highlight their versatility in addressing security challenges across various environments - a benefit that many organizations are already realizing.

Many are already using security locks to secure electronic devices in their organization. The most commonly secured devices include laptops (**44%**), desktops (**43%**), and servers (**42%**), reflecting the priority placed on safeguarding critical hardware that often holds sensitive data. This widespread adoption highlights the recognition of locks as a vital tool in protecting against theft and unauthorized access.

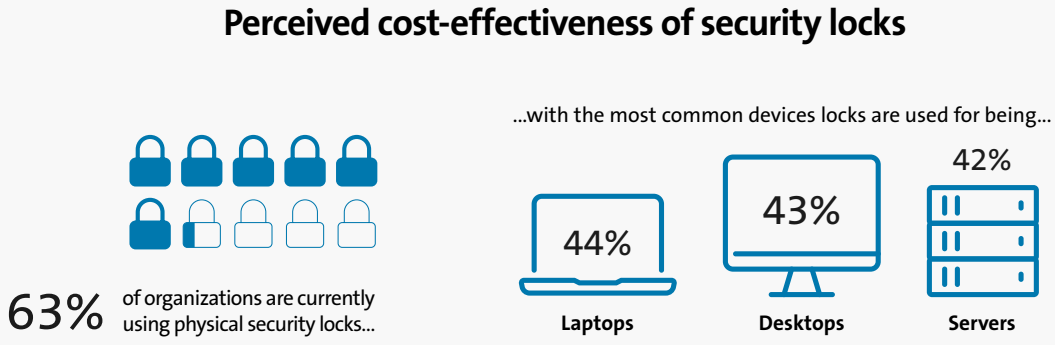


Fig. 7: *For which of the following electronic devices are physical security locks used in your organization? [Asked to all respondents: 1000]*

However, the fact that nearly 4 in 10 of those surveyed say their organizations are not using locks raises concerns about vulnerabilities in device security strategies, especially for devices frequently used in mobile or hybrid working environments.

For organizations, this data underscores the need to evaluate their current security measures comprehensively. While locks are a trusted and widely used solution, expanding their use across a broader range of devices and pairing them with complementary digital protections can help close existing security gaps and mitigate risks more effectively.

Nearly all surveyed (**97%**) recognize the critical role security locks play in helping to prevent theft and the unauthorized access that often follows. This widespread acknowledgment reflects the trust organizations place in physical security as a foundational measure to safeguard devices and sensitive data. Locks act as a frontline defence, reducing opportunities for theft and mitigating risks associated with compromised hardware.

"Having locks in open offices, coworking spaces, or other areas where multiple people may be present **reduces the risk of theft.**"

Board member/C-level; Education – privately owned; 100-249 employees; USA

Pervasiveness of device theft in the last two years, by current working model

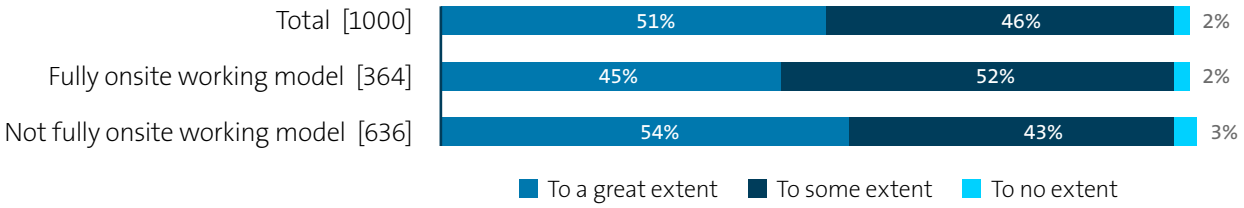


Fig. 8: *To what extent do you believe physical security measures like security locks contribute to preventing device theft which could lead to unauthorized access to company data? [Asked to all respondents, showing data split by type of working model, base numbers in chart]*

This recognition becomes more prominent where organizations have adopted flexible and hybrid working models. In these decentralized environments, devices are increasingly used in unsecured locations, such as home offices or public spaces, amplifying the risk of theft or accidental exposure. Data breaches caused by unsecured devices are significantly more common in the more flexible working setups (**50%** combined vs. **39%** for a fully onsite working model).

Security locks are designed to adapt to diverse environments, offering a reliable safeguard for devices whether they are used in offices, remote workspaces, or public settings, providing organizations with peace of mind across all working models.

The financial consequences of device theft can be staggering, with the cost of replacing stolen hardware often dwarfed by the broader impacts on productivity, regulatory compliance, and data breaches. For organizations, every stolen or unsecured device increases the risk—not just to operations but to the bottom line. Security locks offer a proven and cost-effective solution, trusted by many already in reducing the likelihood of theft and the resulting financial and reputational fallout. By addressing these risks at their root, organizations can take a proactive stance in safeguarding their assets and sensitive data.

While physical security measures like locks are effective, they must be part of a broader strategy to tackle the evolving security risks associated with hybrid working. Combining locks with complementary digital protections, such as encryption and two-factor authentication, ensures comprehensive coverage against both physical and digital threats. Training programs to educate employees on the importance of this integrated approach can further strengthen organizational security. For organizations navigating the complexities of modern working models, integrating physical and digital security measures is essential to minimize risks, protect their workforce, and maintain operational resilience.

Preventing device theft and the resulting data breaches is far more cost-effective than dealing with the aftermath. Taking preventative measures like using laptop locks today can protect your organization from significant financial and operational impacts in the future. To ensure these measures are effective, alignment across senior leadership, management, and teams is critical. A shared commitment to security priorities ensures everyone understands their role in safeguarding valuable assets and reducing risk.

Methodology

Kensington commissioned independent market research specialist Vanson Bourne to undertake the research upon which this report is based. A total of 1,000 senior IT leaders who are involved or have influence over physical IT hardware security in their organization were interviewed in Fall 2024, with representation in the US, UK, France and Germany.

Respondents had to be from organizations with 100 or more employees and from a range of private and public sectors.

The interviews were conducted online and were undertaken using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated, the results discussed are based on the total sample.

About Kensington

Kensington is a leading provider of desktop and mobile device accessories, trusted by IT, educators, business, and home office professionals around the world for more than 40 years. Kensington strives to anticipate the needs and challenges of the ever-evolving workplace and craft professional-tier award-winning solutions for organizations committed to providing peak professionals the tools they need to thrive. The company prides itself as the professionals' choice, and on its core values surrounding design, quality and support.

In office and mobile environments, Kensington's extensive portfolio of award-winning products provide trusted security, desktop productivity innovations, professional video conferencing, and ergonomic well-being.

Headquartered in Burlingame, California, Kensington is the inventor and a worldwide leader in laptop security locks. Kensington is a division of ACCO Brands, the Home of Great Brands Built by Great People, which designs, manufactures and markets consumer and end-user products that help people work, learn and play. In addition to Kensington®, ACCO Brands' widely recognized brands include AT-A-GLANCE®, Five Star®, Leitz®, Mead®, PowerA®, Swingline®, Tilibra and many others. More information about ACCO Brands Corporation (NYSE:ACCO) can be found at www.accobrands.com.

Kensington is a registered trademark of ACCO Brands. All other registered and unregistered trademarks are the property of their respective owners.

All specifications are subject to change without notice. Products may not be available in all markets. Kensington® and Kensington, The Professionals' Choice™ are trademarks of ACCO Brands. All other registered and unregistered trademarks are the property of their respective owners. © 2025 Kensington Computer Products Group, a division of ACCO Brands. k25-4414

FOR MORE INFORMATION CONTACT: sales@kensington.com