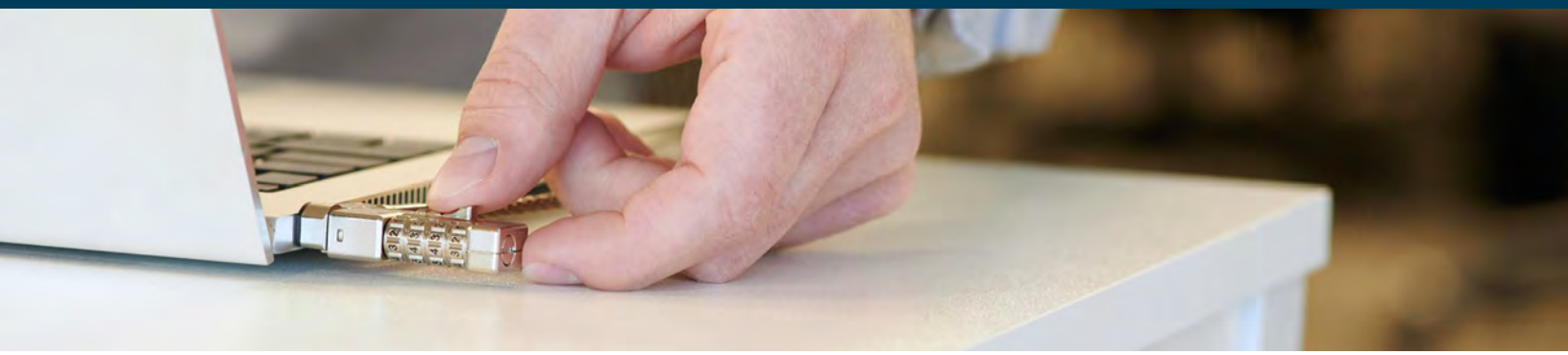
Kensington®

Secure Your Devices, 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 massive shifts in how and where we work. The ultimate driver 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 organisations' physical hardware security throughout the USA and EMEA. Nearly all those surveyed (**92%**) had tightened their security policies in response to the pandemic, recognising the heightened risks associated with decentralised work environments. As we look forward, the proportion of more flexible working models is expected to rise, emphasising 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 unauthorised access to sensitive information, posing significant risks for organisations. With the financial burden of data breaches now totalling millions of dollars every year, the stakes have never been higher. As organisations 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 increased 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 such as security locks can help to mitigate risks and highlight how physical security provides peace of mind in a world in which 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 organisations navigating today's complex security landscape.

Key findings:

76% of respondents say that their organisations have been impacted by incidents of theft in the past two years, incidents being more common in organisations with hybrid working models. For instance, our research revealed that (**85%**) of organisations with hybrid working models experienced an incident of theft in the last two years, compared with **71%** of organisations whose employees work entirely in the office.

The impacts of device theft extend beyond hardware loss, and include:

- 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%**)

Organisations 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).

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

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 (**56%**) than mid-level management (**36%**) to recognise their value.

Almost all those surveyed (**97%**) believe device locks may prevent theft, reducing the likelihood of unauthorised 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 exploitation of critical infrastructure or services. While those examples suggest that cyber incidents are often the most widely discussed – or at least assumed to be – it's important to recognise that physical security threats can be just as critical.

There's little widespread conversation about physical security incidents, where unauthorised 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 organisation has been impacted by incidents of device theft in the past two years.

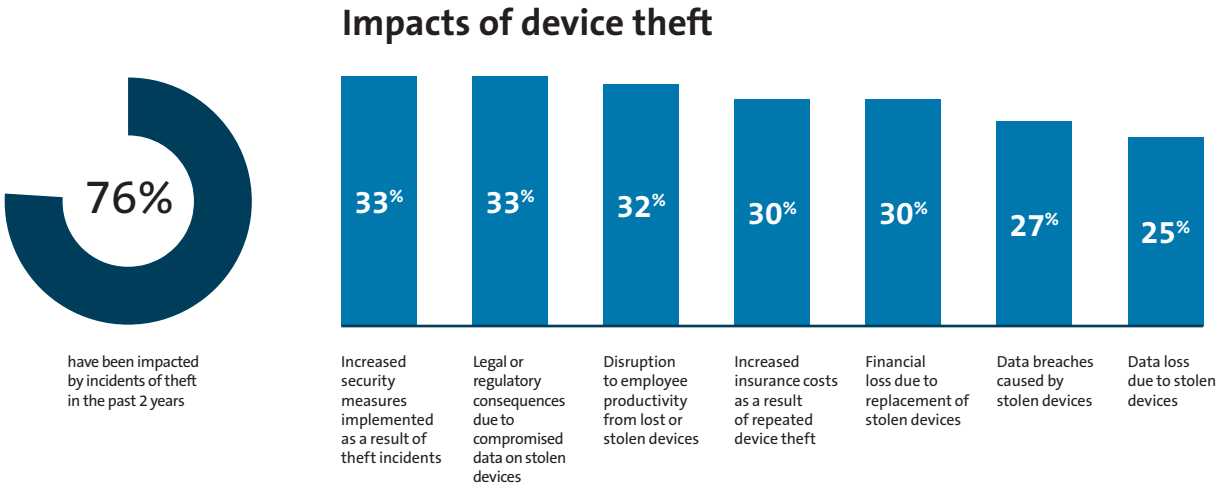


Fig. 1: *How has your organisation been impacted by incidents of device theft in the past two years? [Asked to all respondents: 1,000]*

It's not just the obvious cost of replacing a device that organisations 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, GDPR1 fines can reach up to €20 million or **4%** of an organisation's global turnover, with even less severe violations costing up to €10 million, posing significant financial risks for non-compliance.

Added to the financial impacts is the cost of disruption to employee productivity from lost or stolen devices (**32%**). These impacts also have clear financial and timing consequences on the organisation'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, organisations 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. Every single device theft is a data breach waiting to happen and the financial implications for organisations are staggering. According to IBM's most recent cost of data breach report[2], the global average cost of a data breach in 2024 stood at US$4.88 million, a rise of **10%** in a year from U$4.45 million average in 2023. This figure differs from one industry to another and depending on the size of the organisation, some organisations may face even higher costs.

Spotlight on the data:

- **Sector:** organisations 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 in these businesses exposes them to greater risk of theft
- **Size:** the likelihood of device theft in smaller organisations (100-249 employees) has increased more (**82%**) than in larger organisations with more than 1,000 employees (**69%**), highlighting the relative impact on smaller organisations where resources are more limited and the impacts may be more pronounced
- **Seniority:** Those in more senior positions are much more likely to report that they've been impacted by incidents of thefts (**87%**), than mid-level managers (**67%**). This suggests that those in charge of running the day-to-day of a business are less well-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 at all levels to support a comprehensive security strategy

How do working models play a part here?

We noted the substantial change in ways of working over recent years, the adoption of more flexible working models away from a fixed place of work having been accelerated by the COVID-19 pandemic.

Over three quarters (**76%**) of those surveyed reported that their organisation had been impacted by device theft in the past two years. This become more apparent with hybrid working models – rising to **94%** where employees are fully remote.

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

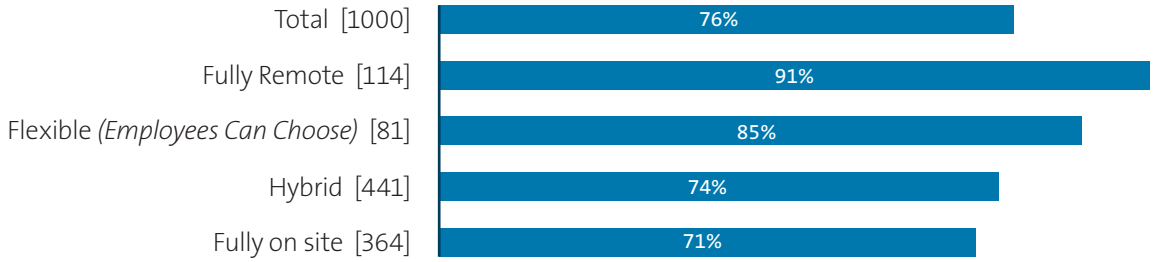


Fig. 2: *Proportion of respondents whose organisation has been impacted by incidents of device theft in the past two years [Asked to all respondents, showing data split by current working model, base numbers in chart]*

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

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

It's important to note that the level of device theft is generally high, even when employees are fully onsite – organisations have no room for complacency, regardless of where their employees work. The device theft threat is nothing new and has not just appeared in the post-pandemic world. 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 public transport (**25%**) and higher 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 organisations 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, unauthorised access and breaches caused by unsecured home networks and decentralised 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

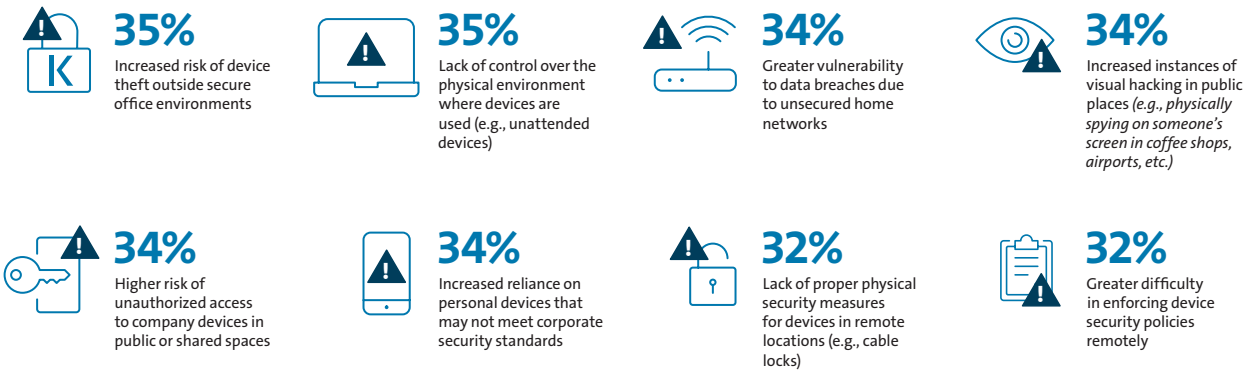


Fig. 3: *In your opinion, what security risks have increased as a result of hybrid or remote working environments following the COVID-19 pandemic? [Asked to respondents whose organisation saw a shift towards hybrid/remote work following the COVID-19 pandemic: 494]*

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 decentralised 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, in 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. Organisations will need to give consideration to protecting their data when employees are out and about, through additional deterrents like privacy screens.

Most concerning areas of device security

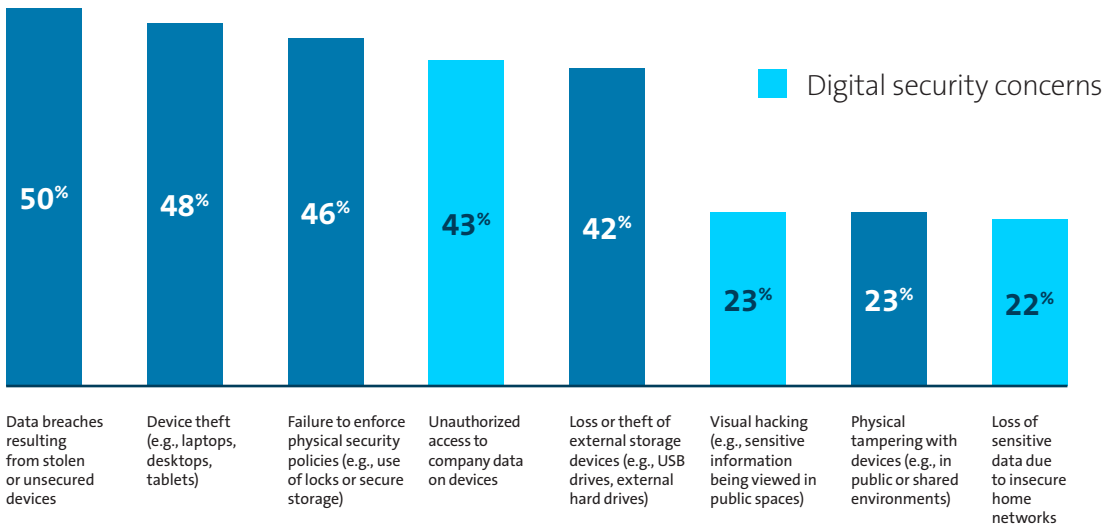


Fig. 4: *Which areas of device security in your organisation concern you the most? [Asked to all respondents: 1,000, showing the combination of responses ranked first, second and third]*

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. Organisations using security locks are **37%** less likely to have experienced a data breach because of an unsecured device than those that do not use them.

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

Fig. 5: *Has your organisation 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 them: 371]*

The outcome is clear: demonstrating a measurable reduction in data breaches or data loss and confirming 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 organisations committed to safeguarding their data and minimising security vulnerabilities.

Spotlight on the data:

- **Sector:** based on survey results, organisations 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. Consumer services were among the most likely to have been impacted by device theft generally. With the latter, this perhaps highlights wider concerns for the decentralised 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 organisations, 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-level or top management 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 sharing of knowledge

"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 organisations look to overcome this?

Organisations are faced with so many digital and physical security concerns - the impacts of device theft are staggering for organisations 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 – and that they offer significant value in preventing theft and breaches. Furthermore, **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?" Organisations may view locks as adding logistical challenges to device management or perhaps a stronger focus on digital over physical security leads to an underestimation of the value of locks, thereby hindering adoption. Yet, when compared to the staggering financial consequences of device theft, the cost of a security lock - typically averaging as little as £24 to £40 per device - represents a minimal investment for reducing risks. Diving into this further, we see clear differences of opinion between the various levels of hierarchy.

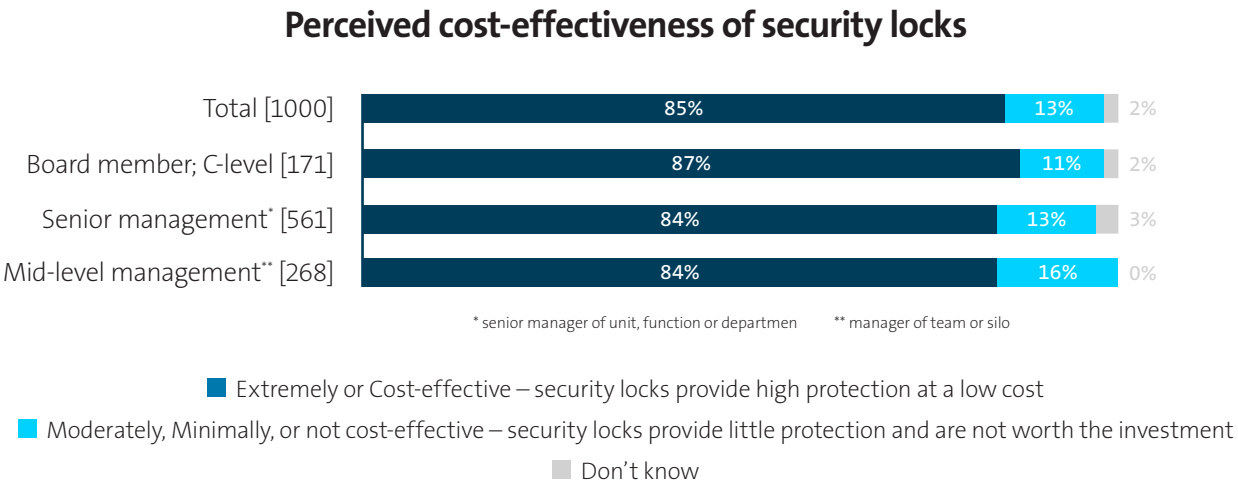


Fig. 6: *In terms of cost-effectiveness, how do you view the role of physical security locks in mitigating potential data breaches or theft? [Asked to all respondents, showing data split by seniority, base numbers in chart]*

These findings emphasise the critical need to address the root causes of device theft and its broader impacts throughout organisations. 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 tend to concentrate on the day-to-day impacts (e.g., productivity loss).

This disconnect highlights the importance of organisational 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 [the corporate device] 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 organisations are already realising.

Many are already using security locks to secure electronic devices in their organisation. 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 unauthorised access.

Perceived cost-effectiveness of security locks

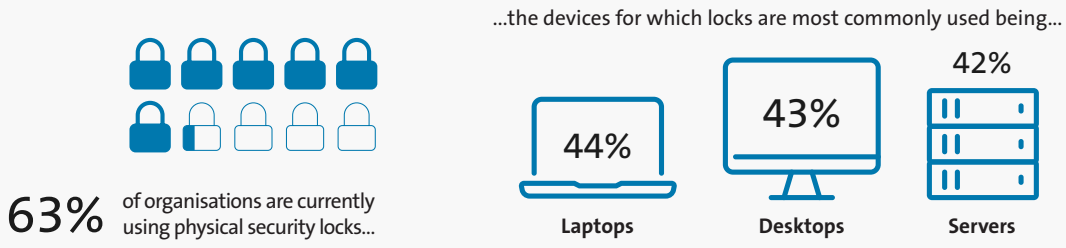


Fig. 7: *For which of the following electronic devices are physical security locks used in your organisation? [Asked to all respondents: 1,000]*

However, the fact that nearly **40%** of those surveyed say their organisations are not using locks raises concerns about vulnerabilities in device security strategies, especially for devices frequently used in mobile or hybrid working environments.

For organisations, these data underscore 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 those surveyed (**97%**) recognise the critical role security locks play in helping to prevent theft and the unauthorised access that often follows. This widespread acknowledgment reflects the trust organisations place in physical security as a basic 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, co-working spaces, or other areas where a number of people may be present **reduces the risk of theft.**"

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

Belief that physical security measures contribute to preventing device theft

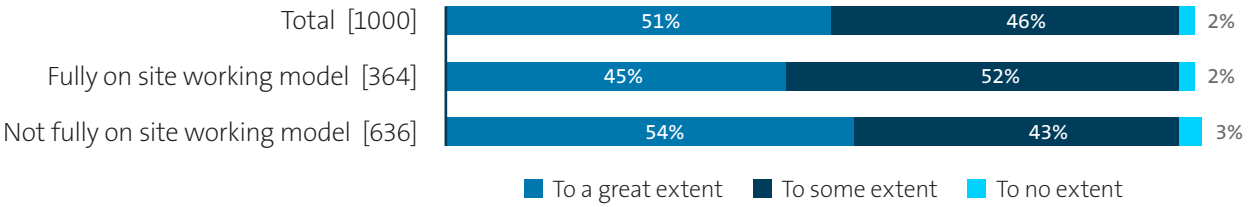


Fig. 8: *To what extent do you believe physical security measures like security locks contribute to preventing device theft which could lead to unauthorised access to company data? [Asked to all respondents, showing data split by type of working model, base numbers in chart]*

This recognition becomes more prominent where organisations have adopted flexible and hybrid working models. In these decentralised 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 organisations 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 organisations, 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, organisations can take a proactive stance in safeguarding their assets and sensitive data. While physical security measures such as 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 protection such as encryption and two-factor authentication, ensures comprehensive coverage against both physical and digital threats.

Training programmes to educate employees on the importance of this integrated approach can further strengthen organisational security. For organisations navigating the complexities of modern working models, integrating physical and digital security measures is essential to minimise 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 preventive measures like using laptop locks today can protect your organisation 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 with or have influence over physical IT hardware security in their organisation were interviewed in the autumn of 2024, with representation in the USA, UK, France and Germany.

Respondents were from organisations 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 organisations committed to providing peak professionals with the tools they need to thrive. The company prides itself on being 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 recognised 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.

FOR MORE INFORMATION CONTACT: contact@kensington.com

Kensington
The Professionals' Choice™