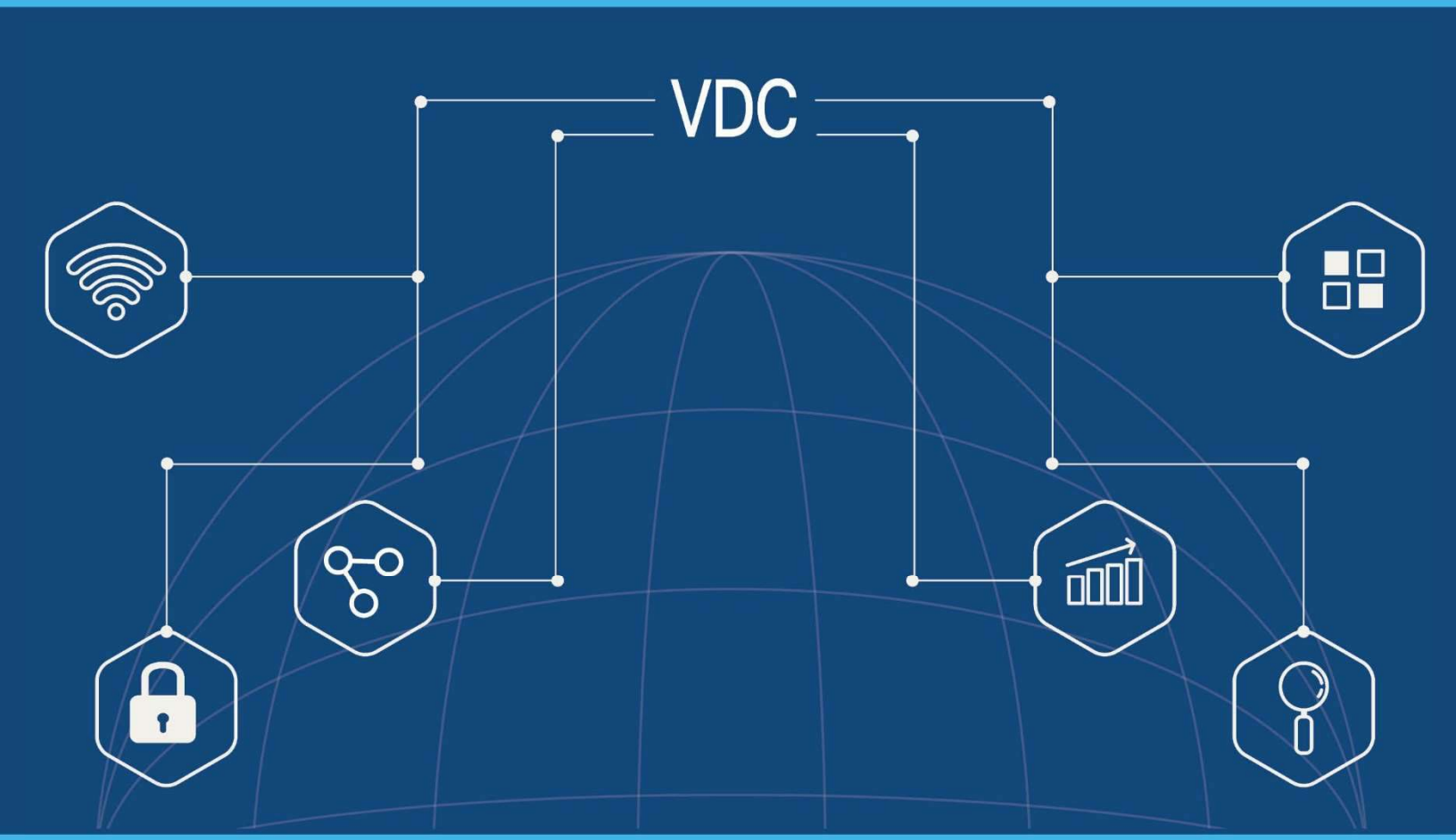
Securing OT with Purpose-built Solutions



Licensed to Distribute by:

kaspersky

VDC Research

by Jared Weiner, Director

Chris Rommel, Executive Vice President

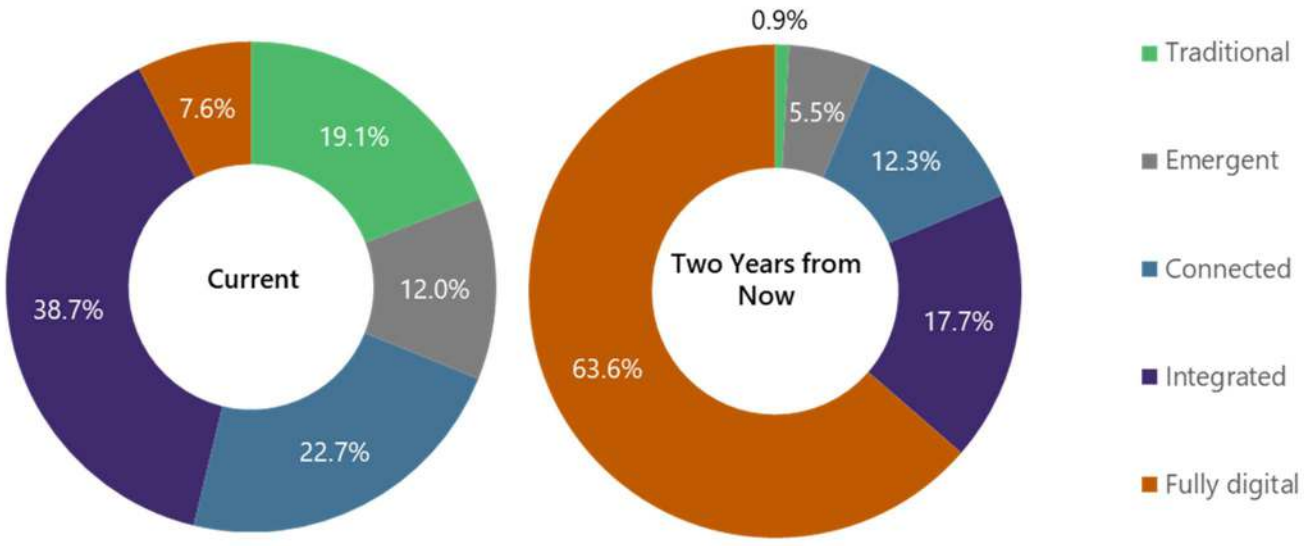
Introduction

In recent years, organizations across all industrial and manufacturing subsectors have embraced digital transformation strategies to combat steadily intensifying economic and financial pressures. Though the complexity of deploying digital technologies in diverse operational environments has, thus far, engendered a gradual transition, results from a recent survey[1] demonstrate that the "fully digital" era is nearly upon us. Nearly two-thirds of respondents expect their organizations to be fully digital two years from now, versus less than 8% today [See Exhibit 1]. Though the ultimate pace of transition may take time to fully manifest, the rapid maturation of digital-enabling technologies such as IoT connectivity and edge computing has significantly accelerated industrial organizations' digital transformation efforts – as well as their need to understand the scale of both the new opportunities and risks it presents.

8 times as many organizations expect to be "fully digital" within the next two years

Exhibit 1: Organization's Current and Expected Digital Transformation Status[2]

(Percentage of Respondents)



In operational technology (OT) environments, digital technologies span a broad range of operational objectives and processes. By adopting digital technologies and uniting various enterprise and operational data sources, organizations can make real-time, data-driven decisions that significantly improve operational efficiency,

[1] See *Background on VDC Research* section for details.

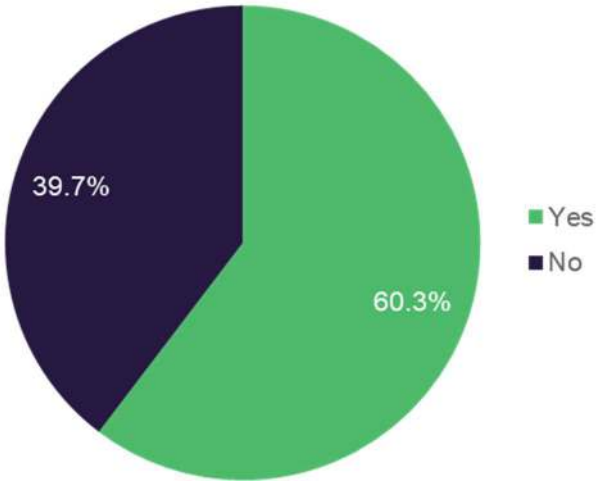
[2] Traditional–mostly/entirely reliant on manual processes; Emergent–beginning to adopt digital technologies for specific tasks; Connected–multiple connected digital technologies; Integrated–high levels of automation and connectivity throughout the organization; Fully digital–proactive, continuous improvement of digital capabilities.

productivity, and worker safety. For example, digital systems for asset, maintenance, and supply chain management have become common tools for minimizing operational expenses, while advanced solutions such as those for digital twins and smart manufacturing have gained momentum among OT organizations focused on process and production optimization. Regardless of the use case, digital technologies rely massively on data from machines, sensors, and other interconnected data sources to be effective. The connectivity required to facilitate the exchange of this data exposes OT systems and networks—traditionally isolated from the outside world—to considerable cybersecurity risks.

OT organizations that fail to adequately address these risks in their haste to attain transformative business outcomes leave themselves exposed to the potentially severe consequences of a cybersecurity breach. Breaches are particularly troubling in OT environments, where system failures can result in life-threatening or otherwise catastrophic situations. Combined with the financial and operational implications of shutting down operations—lost production, scheduling delays, scrap, overhead—the consequences of even a temporary disruption can be disastrous. Among our survey respondents, more than 60% indicated that cybersecurity breaches in 2023 and 2024 had caused their organization to incur costs [See Exhibit 2].

Exhibit 2: Cybersecurity Breaches Caused Organization to Incur Costs

(Percentage of Respondents)

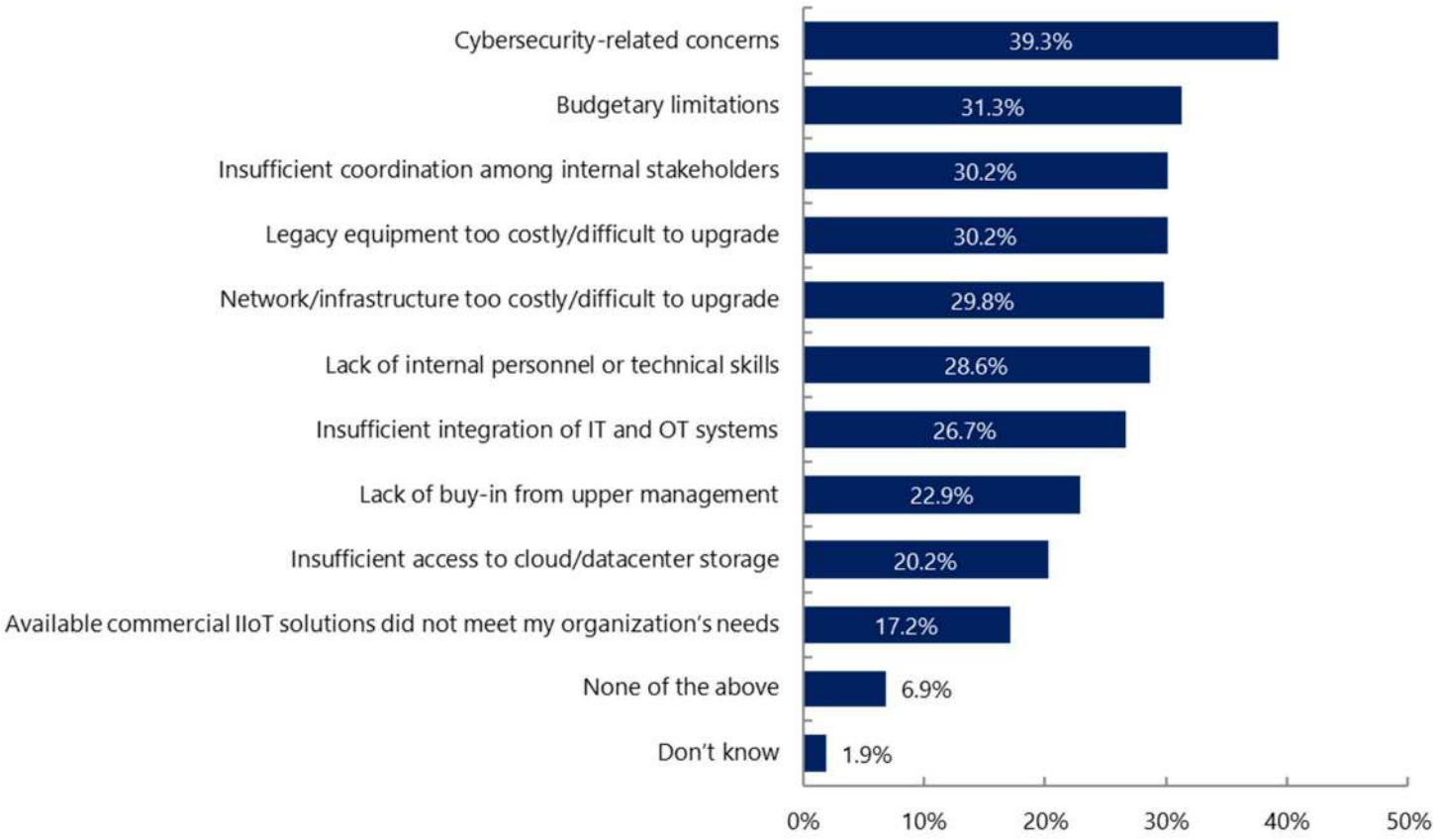


Accordingly, cybersecurity-related concerns were identified as the most common factor negatively affecting their organization's ability to implement digital technologies in its OT environment [See Exhibit 3]. The specific cybersecurity-related concerns slowing respondents' digital technology adoption, shown in Exhibit 4, spanned many potential pitfalls, hinting at the breadth and depth of cybersecurity challenges faced by OT organizations pursuing digital transformation. These cybersecurity challenges expose the need for change. With connected OT systems playing an increasingly important role in enterprise-wide operations, finding ways to effectively and efficiently manage cybersecurity risk has emerged as an acute need. Over the course of this paper, we will

highlight key trends and opportunities for risk mitigation and cost savings when planning your next OT solution implementation.

Exhibit 3: Factors Negatively Affecting Organization's Ability to Implement Digital Technologies in its OT Environment

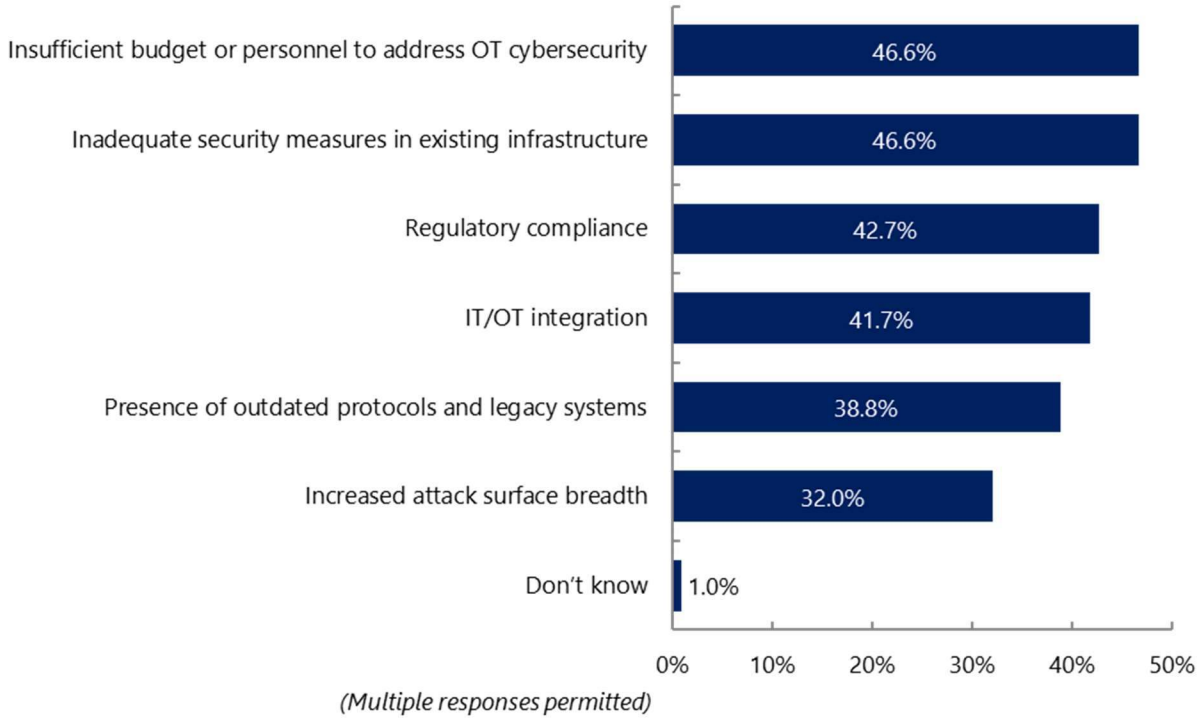
(Percentage of Respondents)



(Multiple responses permitted)

Exhibit 4: Cybersecurity-related Concerns Negatively Affecting Organization's Ability to Implement Digital Technologies in its OT Environment

(Percentage of Respondents)



(Multiple responses permitted)

Background on VDC Research

VDC has covered industrial and other business-to-business technology markets since 1971. The analysis and supporting discussions in this paper are based on VDC's ongoing research in the OT cybersecurity market and by findings from a survey of more than 250 OT and IT decision makers familiar with the OT cybersecurity practices within their respective organizations. This survey offers insight into leading business and technical trends affecting OT organizations as well as the best practices implemented to address them. Respondents span a range of industries including energy and utilities, transportation and logistics, and manufacturing sub-sectors such as chemicals and pharmaceuticals, among others.

OT Cybersecurity Can Be Overwhelming

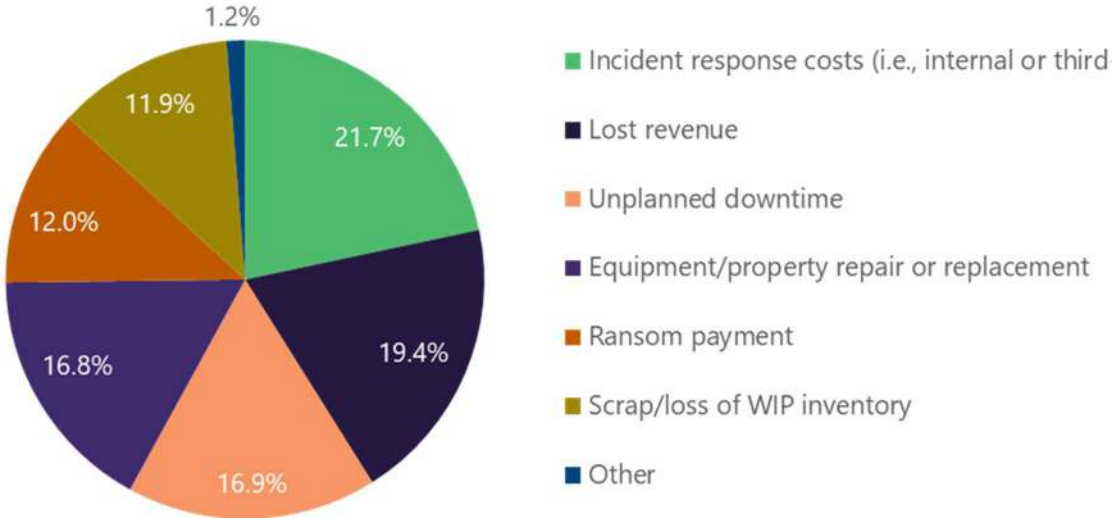
The Financial Implications of a Breach Can Be Devastating

Nearly 25% of OT decision makers report cyberattack-related financial damages of more than $5 million per incident

The financial consequences of an OT cybersecurity breach are multi-faceted and multivariate. To understand the total financial impact of a breach, organizations must consider not only breach-related costs (such as those for incident response or ransom payments), but also those associated with lost revenue opportunities, lost production time, scrap and lost work-in-progress inventory, and damaged equipment or property. Accounting for each of these cost categories, nearly 25% of our survey respondents estimated cyberattack-related financial damages of more than $5 million per incident across 2023 and 2024. The distribution of these costs, as shown in Exhibit 5, is also subject to variance by region, industry, and various other organizational characteristics. Beyond these known and quantifiable costs, OT organizations in service-oriented sectors may also face significant reputational damage or legal consequences due to service outages or broken contracts.

Exhibit 5: Distribution of Costs from Cybersecurity Breaches

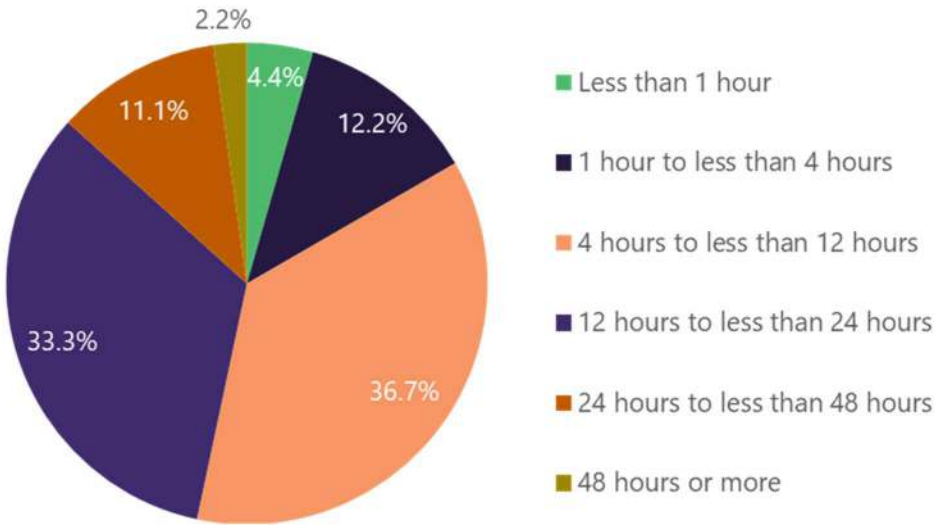
(Percentage of Respondents)



Negatively affecting production output, customer delivery schedules, and many other internal and external profit drivers, unplanned downtime has become a critical metric for OT organizations deploying digital technologies to improve their bottom line. Though OT organizations have increasingly leveraged condition monitoring and other maintenance-driven strategies to combat unplanned downtime, actions that improve cybersecurity posture—which can reduce downtime by minimizing the risk of breaches that cause equipment failure—are often overlooked. The link between cybersecurity and unplanned downtime is clear. In fact, cybersecurity breaches most commonly caused unplanned downtime lasting anywhere from 4 to 24 hours [See Exhibit 6]. Considering that unplanned downtime can cost organizations thousands or even millions of dollars every hour, OT organizations cannot afford to ignore cybersecurity in their pursuit of downtime elimination.

Exhibit 6: Estimated Length of Production Interruption Caused by Cybersecurity Breaches

(Percentage of Respondents)



Patching OT Systems is a Complex Challenge

Unfortunately, OT environments are notoriously difficult to protect. For example, while IT systems are generally updated and patched at regular, sometimes automatic intervals, patch management for OT devices is a significant challenge [See Exhibit 7]. OT system updates must be carefully planned and coordinated to minimize operational downtime. However, many organizations struggle to find or prioritize time to halt operations and roll out patches. This leads to patching practices that are woefully inadequate [See Exhibit 8]. In fact, most organizations patch their systems only every few months or longer—a risky timeline for organizations exposed to a rapidly evolving threat landscape. Patches are also challenging to manage in OT environments due to the combination of poor device visibility, inconsistent availability of patches from vendors, the specialized expertise necessary to work on so many different proprietary systems, and regulatory compliance requirements. Furthermore, the criticality of these systems necessitates extensive testing prior to deployment to ensure safety

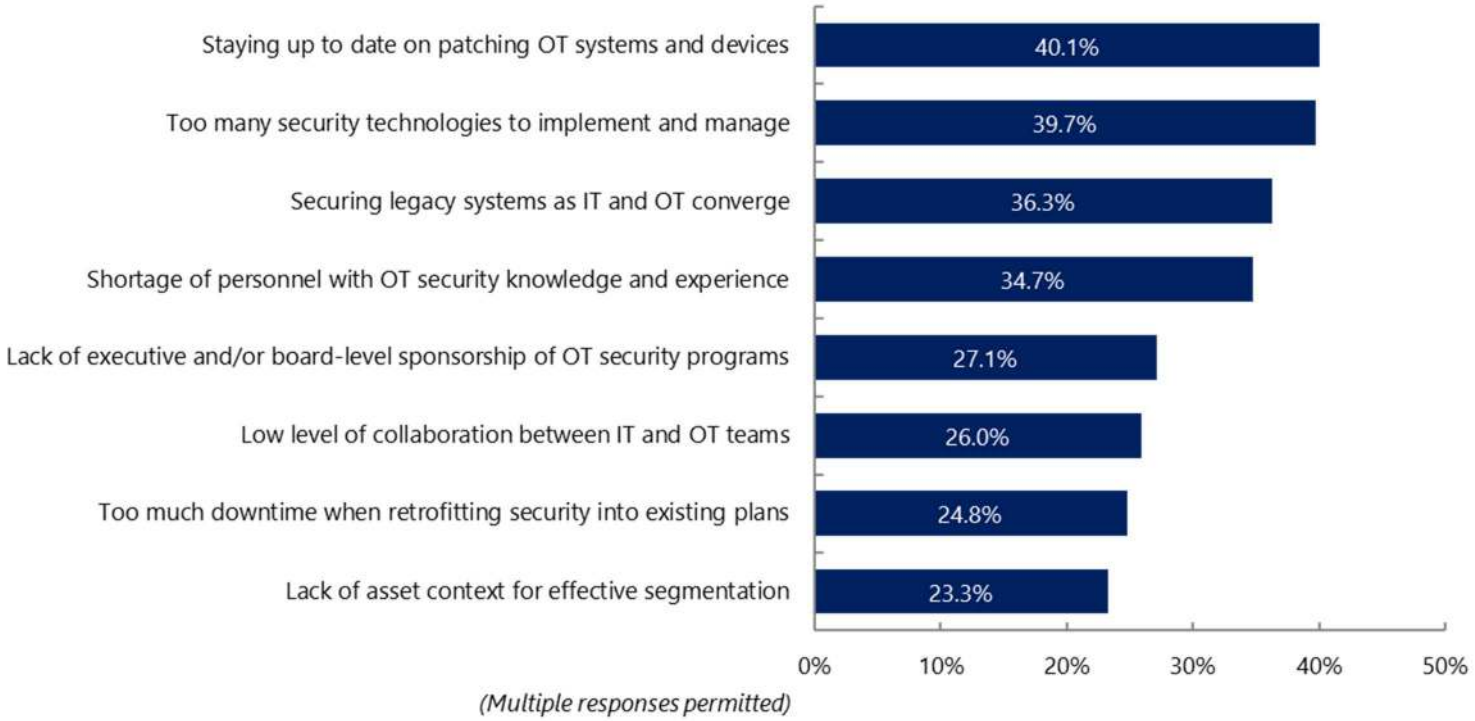
and stability. Organizations without sound cybersecurity practices and technology/solutions place themselves at risk.

The growing presence of IoT devices is significantly expanding the OT attack surface

Navigating OT/IT convergence is similarly daunting for many organizations. The convergence of OT and IT requires merging traditionally disparate systems built predominantly using proprietary technologies rather than open standards. The sudden proliferation of IoT devices—cameras, smart sensors for asset tracking and machine health monitoring, smart climate controls, etc.—has added another layer to the convergence challenge. These IoT devices can be difficult to efficiently identify, patch, and manage on an ongoing basis. Their growing presence significantly expanding the attack surface for industrial organizations. The wireless nature of many of these devices provides an additional layer of risk and further complicates these device management challenges. Accordingly, CISOs and other cybersecurity leaders have been increasingly called upon to manage cyber resiliency across these formerly separate domains. However, many CISOs have limited experience working in these environments, amplifying the risk of breaches, downtime, and ballooning remediation costs.

Exhibit 7: Biggest OT Security Challenges

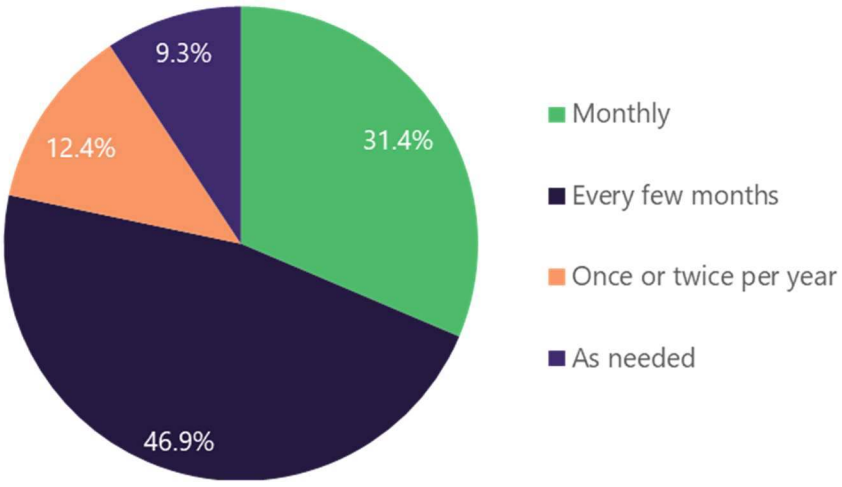
(Percentage of Respondents)



(Multiple responses permitted)

Exhibit 8: Frequency with which Organization Patches Vulnerabilities within its OT Environment

(Percentage of Respondents)



Widening Skills Gap Strains In-house OT Cybersecurity Capabilities

Designing, implementing, and managing an effective OT cybersecurity strategy requires dedicated personnel with unique skillsets combining cybersecurity expertise and experience working in operational environments. While this skillset has long been elusive, recent employment trends have exacerbated the problem. In fact, more than one-third of survey respondents cited this skills gap among their biggest OT cybersecurity challenges [See Exhibit 7]. In addition, highly trained employees are more likely to change jobs than they were decades ago. These employees take their expertise with them when they leave, creating continuity challenges and leaving organizations unable to effectively or efficiently gauge cybersecurity posture or address cyber risk.

The OT cybersecurity skills gap is easily addressed with the selection of an OT cybersecurity vendor partner

Budgetary constraints have provided an additional barrier to building an in-house cybersecurity team, particularly among small- to medium-sized organizations. Despite organizations steadily embracing the notion that they cannot afford to leave their OT environments unsecured, many have been unable to address OT cybersecurity concerns themselves due to their lack of in-house expertise. As such, these organizations have found tremendous value in leveraging the skills and experience of OT cybersecurity vendors. With the skills gap likely to endure and even expand as industrial cybersecurity considerations and requirements intensify, the need for OT organizations to engage with experienced OT cybersecurity vendors is more important than ever.

Pursuing Cyber Resilience with Specialized Solutions

OT organizations can address many of their OT cybersecurity objectives by deploying specialized cybersecurity hardware, software, and services intended for converged operating environments. Two of the leading software categories within the OT cybersecurity software ecosystem are asset/network visibility solutions (such as Kaspersky Industrial CyberSecurity for Networks, which are useful for network traffic analysis, detection and response) and endpoint protection solutions (such as Kaspersky Industrial CyberSecurity for Nodes, which are vital tools for securing critical endpoints). Among our survey respondents, the use of these technologies indicated an organization with mature cybersecurity practices and fewer cybersecurity breaches, as shown in Exhibits 9 and 10.

Exhibit 9: Maturity of Organization's OT Cybersecurity Policies and Practices

(Average of Responses)

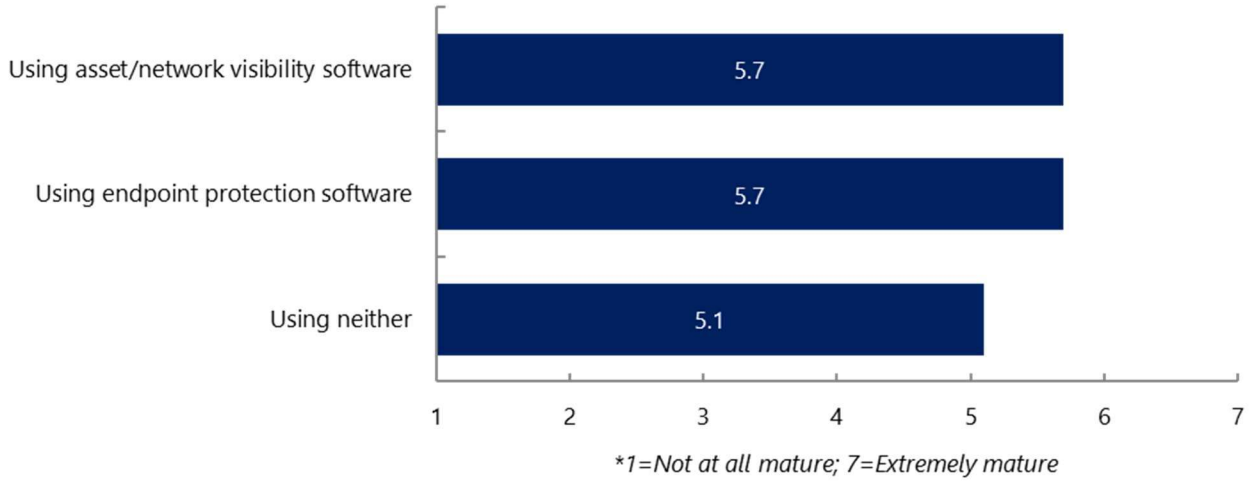
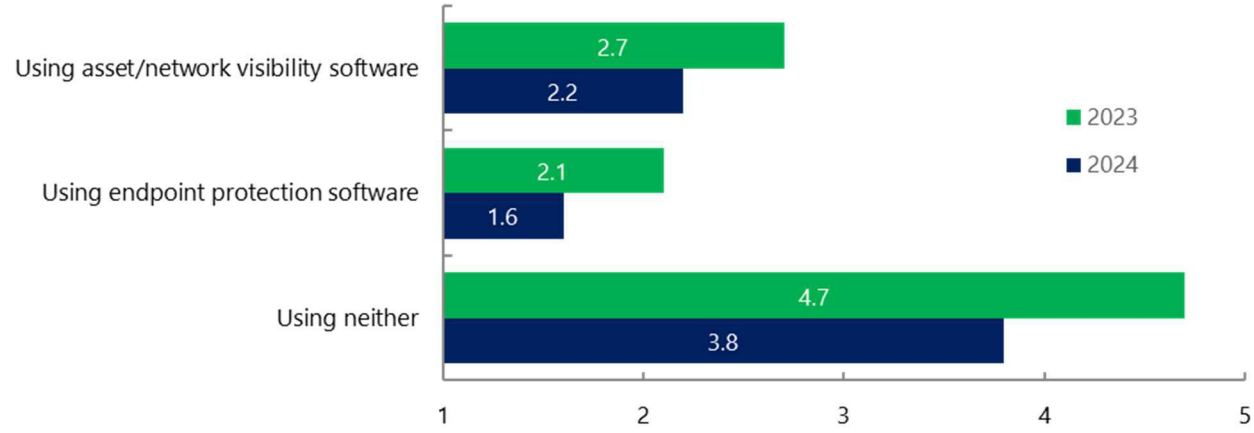


Exhibit 10: Number of Cybersecurity Breaches that Affected Organization's Operations in 2023 and 2024

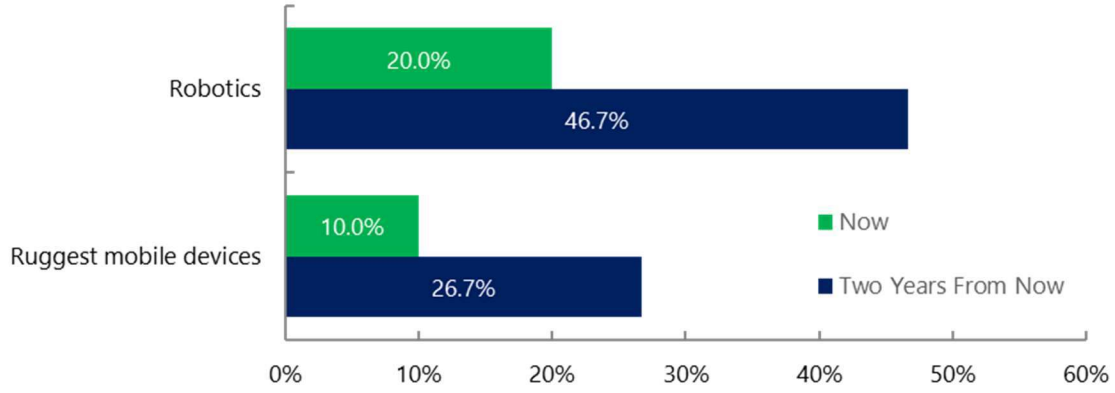
(Average of Responses)



While the use of any commercial OT cybersecurity solution is commendable, the most resilient organizations are those guided by the cybersecurity concept Defense in Depth, which preaches the importance of implementing multiple layers of cybersecurity to maximize resiliency. The notion of "designing for security" has also become quite common, with cybersecurity-conscious OT organizations showing a growing preference to deploy networking technologies with built-in OT cybersecurity protection. These fundamental cybersecurity best practices are particularly critical when considering the degree to which digital transformation has introduced new connected equipment and systems to organizations' operating environments, rapidly expanding their attack surface. Within the energy and utilities sector, for example, usage of mobile devices and robotics is expected to increase dramatically over the next two years [See Exhibit 11]. End-to-end security coverage and the secure-by-design methodology are essential for safeguarding these heterogeneous, highly interconnected IT, OT, and IIoT systems. Solutions that provide fault-tolerant and secure networks—such as Kaspersky SD-WAN—are another category of tool adding critical protection across these environments.

Exhibit 11: Digital Technologies Used or Deployed within Organization's OT Environment (Energy and Utilities sector)

(Average of Responses)



**Not all responses shown.*

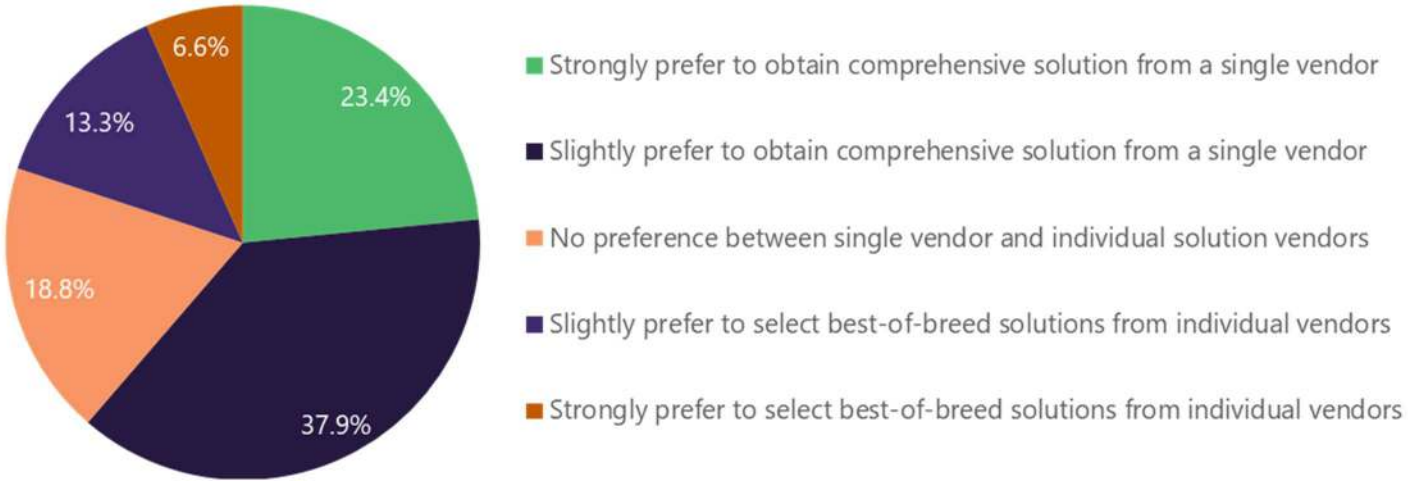
Unfortunately, many OT organizations consider implementing and managing multiple cybersecurity technologies to be a significant challenge, as shown previously in Exhibit 7. In fact, more than 60% of respondents preferred obtaining comprehensive OT cybersecurity solutions from a single vendor rather than obtaining multiple best-of-breed solutions from individual vendors [Exhibit 12]. While vendor consolidation is hardly a new strategy, the importance of simplifying OT environments and easing integrations with other OT and enterprise systems has become especially critical as organizations digitalize their operations. OT organizations can address these challenges by working with enterprise-grade cybersecurity vendors, such as Kaspersky, that unify IT, OT, and IIoT

60% of organizations recognize the value in obtaining comprehensive OT cybersecurity solutions from a single vendor

cybersecurity coverage within a single, end-to-end platform. Moreover, this single platform approach can help organizations address personnel shortages, as natively integrated solutions reduce the workload for in-house cybersecurity teams.

Exhibit 12: Extent to which Organization Prefers to Obtain OT Cybersecurity Solutions as a Comprehensive Solution from a Single Vendor versus Selecting Best-of-Breed Solutions from Multiple Vendors

(Average of Responses)



Purpose-built Solutions Deliver Significant Savings

The OT cybersecurity ecosystem is a diverse market with a wide range of solutions that can help OT organizations minimize the costly repercussions of a cybersecurity breach. Many different factors influence organizations' evaluation and selection of specific OT cybersecurity solutions. These organizations are mostly guided by internal operating requirements and previously identified best practices, however, external factors such as region- or industry-specific regulatory requirements (e.g., NIS2) are also critical drivers. Enterprise requirements (i.e., compatibility with existing enterprise systems supporting various business and operational functions) have also become increasingly influential. Despite the uniqueness of every organization's operational and enterprise requirements, certain trends and conclusions become apparent when comparing organizations with similar characteristics.

There are many different costs and variables that impact the cost savings an OT cybersecurity solution can provide to an organization, such as the number of breaches prevented, the time and cost associated with remediating breaches, the cost of unplanned downtime, and the cost of ransom payments, among others. Of note, more than 50% of respondents indicated their organizations do not use an ROI or risk calculator when justifying their OT cybersecurity budgets. Organizations that do utilize such resources can put themselves ahead of their competitors. Our research results highlight a few of the significant cost savings available across these dimensions when organizations invest upfront in purpose-built OT cybersecurity solutions, such as those offered by Kaspersky.

Most notably, organizations that use solutions for asset/network visibility and endpoint protection can expect significant cost savings. Not only does the use of these technologies independently reduce breaches, but our research results show even greater improvements for those organizations using both technologies together. Furthermore, breaches among organizations using neither asset/network visibility nor endpoint protection were more likely to incur costs than for organizations using either technology. For example, a global organization in the Energy & Utilities industry with between 2,500 and 9,999 employees would have reduced its breach-related losses by more than 30% if it had deployed asset/network visibility and endpoint protection solutions in its OT environment [See Exhibit 13].

An Energy & Utilities company would have reduced costs by losses by one third with the use of asset/network visibility and endpoint protection solutions

Exhibit 13: Cost Savings Calculation for Mid-sized, Global Energy & Utilities Operator

	Your Organization[1]	If You Had Used Asset/Network Visibility	If You Had Used Endpoint Protection	If You Had Used Asset/Network Visibility AND Endpoint Protection[2]	If You Had Used Threat Remediation & Response Services
Number of breaches in last year	4	2	2	2	3
Number of breaches resulting in financial loss	3	1	1	1	2
Estimated cost of breach-related losses	$1,000,000	$682,399	$800,066	$666,295	$874,833
Total savings		**$317,601**	**$199,934**	**$333,705**	**$125,167**
Savings %		32%	20%	33%	13%

[1]Organization's attributes: industry- energy and utilities; operating region- global; company size- 2,500 to 9,999 employees
[2]Note: Savings calculated for individual solution categories are not additive. As such, the total from this column may be less than the combined total of the individual calculations.

OT cybersecurity services—such as those for threat remediation and response—are also highly effective in reducing the cost of cybersecurity breaches. Through such services, vendors leverage their cybersecurity and OT expertise to help OT organizations control breach-related expenses by identifying, containing, and eradicating malicious activity and quickly enabling a return to normal operations. For example, a pharmaceutical manufacturer in EMEA with between 500 and 2,499 employees would have reduced its breach-related losses by 75% if it had utilized threat remediation and response services for its OT environment [See Exhibit 14].

A pharmaceutical company would have saved $750,000 with threat remediation and response services

Exhibit 14: Cost Savings Calculation for Small Pharmaceutical Manufacturer in EMEA

	Your Organization[1]	If You Had Used Asset/Network Visibility	If You Had Used Endpoint Protection	If You Had Used Asset/Network Visibility AND Endpoint Protection[2]	If You Had Used Threat Remediation & Response Services
Number of breaches in last year	4	1	2	1	2
Number of breaches resulting in financial loss	3	1	1	1	1
Estimated cost of breach-related losses	$1,000,000	$435,438	$619,254	$476,435	$251,474
Total savings		**$564,562**	**$380,746**	**$523,565**	**$748,526**
Savings %		56%	38%	52%	75%

[1]Organization's attributes: industry- pharmaceutical manufacturing; operating region- EMEA; company size- 500 to 2,499 employees
[2]Note: Savings calculated for individual solution categories are not additive. As such, the total from this column may be less than the combined total of the individual calculations.

VDC's View: Summary & Recommendations

OT Cyber Risk Is Too Consequential to Ignore

While IT-related breaches are decidedly impactful, the stakes are considerably higher in OT environments, where system failures can result in serious physical consequences such as property or equipment damage, environmental damage, injury, and even death. Also accounting for financial implications—which include direct expenses such as ransom payments, penalties, and remediation as well as indirect costs such as lost production and reputational damage—OT organizations simply cannot afford to ignore cybersecurity. By adopting modern OT cybersecurity strategies and deploying robust OT cybersecurity solutions, OT organizations can minimize their risk while maximizing their bottom line.

Complex Environments Require Proven Expertise and Holistic Portfolio

The complexity of OT environments is such that most organizations are unable to design, deploy, and manage an effective cybersecurity strategy on their own. Widening expertise gaps and persistent labor challenges have exacerbated this problem in recent years. Our research shows that organizations that have adopted formal OT cybersecurity solutions have less risk and incur fewer costs than organizations without formal solutions in place. By leveraging the IT, OT, and IIoT expertise of cybersecurity vendors such as Kaspersky, OT organizations can be confident that their operations are covered by robust, purpose-built cybersecurity technologies. Furthermore, by working with a proven vendor offering end-to-end coverage in a single, native platform, these organizations can also simplify their OT environment and improve integrations with enterprise systems.

Identify Partners with Hybrid OT and Cybersecurity Expertise

OT environments, heterogeneous by nature, comprise a wide range of devices, machinery, and systems that vary considerably from industry to industry. Industrial operators are also commonly governed by regulatory requirements specific to individual sectors or geographic regions. The NIS2 Directive, for example, requires companies of a certain size operating in energy, manufacturing, and other critical sectors within the European Union to adopt a baseline set of security measures to protect against cyber threats. This directive, like many other regulatory mandates, is a complex challenge for OT organizations to navigate, especially considering the consequences of non-compliance, which may include monetary or even criminal penalties. As such, OT organizations should look for cybersecurity partners that understand not only the unique requirements of their operating environment, but also the evolving regulatory guidelines that organizations must follow to remain in compliance. Mature cybersecurity vendors, such as Kaspersky, will also enable robust patch management for all devices in an organization's OT environment, including precise vulnerability information as well as insights into the current threat landscape and recommendations for protection when patching is not feasible.

Pursue the Next Step of IT/OT Cyber Resilience

While existing IT/OT systems certainly require protection, OT organizations must consider the Secure by Design ideology when implementing new OT devices or systems. Secure by Design products—such as cyber immune products based on KasperskyOS, which adhere to specific development methodologies and architecture requirements—remain resilient under attack, can resist exploits of unknown vulnerabilities, and require minimal attention in terms of patching and external protection. By leveraging this methodology, organizations can improve their systems' resilience with minimal additional cybersecurity costs, thereby reducing total cybersecurity expenses in the long run.