The Voice of the Customer, 2022

A Benchmarking Survey

"Increasing the business value of physical security in uncertain times"

convergint®

Introduction

Convergint is a global systems integrator focused on delivering results for our customers through unparalleled service excellence. You are our number one priority therefore we continuously seek out opportunities to add value. Recognizing the absence of peer-to-peer benchmarking in security, Convergint Research & Insights conducted its first Customer Experience survey in 2022, gathering cross-industry information to provide you with insights regarding:

- Trends in security staffing, organizational structure, and procedures
- Trends in security budgeting, financing, and procurement
- Trends in innovation and technological adoption within the security space

Our goal is to provide you with information that supports your own security planning and offer considerations to become a true business enabler.

convergint

Current Market Conditions:

The global pandemic has been a challenge for virtually all businesses since 2020. The outlook for 2023 is no less complicated given economic uncertainty, global conflicts, and civil unrest. As such, many businesses are spending with caution.

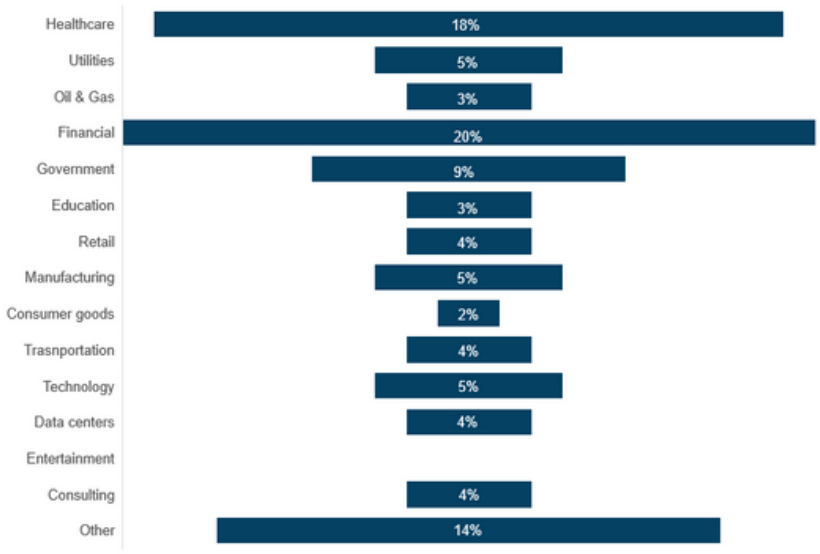
The workplace itself is weathering an uptick in incidents of physical violence and a growing cyber threat. Furthermore, many organizations are adopting a 'flexible workplace' instead of mandating a full-time return-to-work initiative. All in all, security teams are juggling numerous challenges and opportunities.

They now have a seat at the table for discussions of real estate footprints and office utilization as they manage a safe return to work for their colleagues. Subsequently, security teams may be spearheading costs savings for organizations and thereby showing the sustainable value inherent in their department.

In addition, the ongoing digital revolution is providing security leaders with yet another opportunity to showcase the business value of security. A cloud centric architecture and outsourcing certain security services can ease the pressure off already overburdened staff and create full focus on core business activities.

Survey Participants

For this benchmarking survey, Convergint conducted interviews with senior physical security practitioners in a wide array of industries including:



As indicated, finance/banking, healthcare, and government were most represented in results.

Survey Results

The Security Organization

Where does security fit in the context of the overall organization?

- Security teams most commonly fall under Facilities or a stand-alone Security department.
- Security has become elevated in organizational importance as evidenced by survey responses. 25% of participants now report directly to the CEO, while another 10% report to other C-level executives including Vice Presidents.

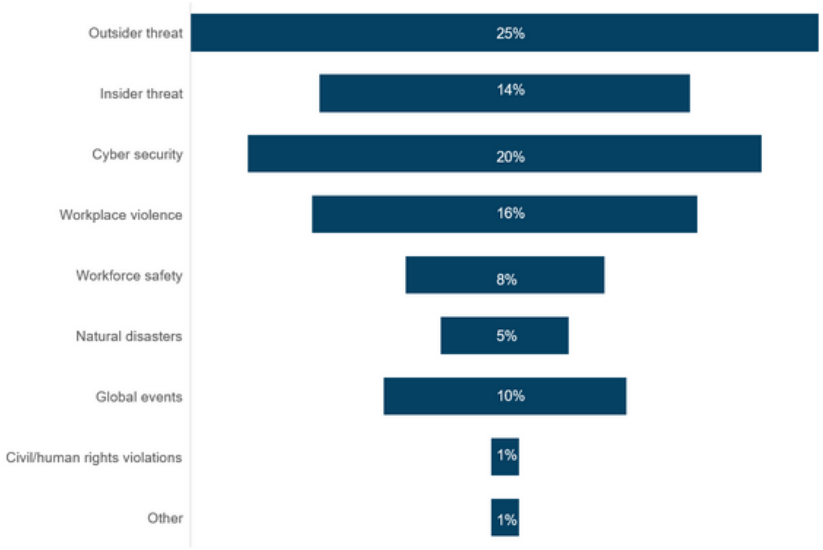
Insight: Despite their increasing prominence, many respondents are challenged in articulating how security aligns with bigger picture business strategy or how their team communicates value to the organization. This is a stark contrast with the clarity with which they identify a common departmental objective: to provide a safe and secure work environment for employees, visitors, and customers.

What are the biggest security threats being managed?

Respondents noted three primary threats to their organizations overall:

- Outside threat (unauthorized access, theft, burglary, vandalism)
- Cyber security
- Workplace violence

convergint



Not surprisingly, vertical challenges played into responses. As an example, utilities cited natural disasters as the greatest threat to their organizations whereas finance/banking called out global events like the economic climate and the pandemic.

Assessing Change

Cyber: 24% of respondents believe cyber security will have an increased impact on their teams going forward, and the blurred lines between security and IT will dictate that security teams onboard personnel with more intensive IT skills.

Reporting: Only 5% of respondents see utilizing data for business support and processes as an opportunity to show business value for the security department. This data point indicates little forward movement.

Resources: Hiring challenges and retaining talent remain a huge struggle for most security teams. Furthermore, issues in securing and retaining personnel has increased pressure on existing staff.

Roles: 72% of participants anticipated that their roles would change in the upcoming 1-2 years, reflecting the growth and fluidity within security organizations.

Supply Chain: Global supply chain issues have impacted many organizations and how they conducted business across all functions. Security is no exception.

Systems: System standardization across the board promises to be a huge focus for the upcoming 1-2 years. This combines with true integration of disparate access control and video systems to better utilize physical security data for business value purposes.

Pandemic Impacts

Workplace Model

Return-to-office initiatives have not been mandated by upper management according to most respondents. As such, a hybrid workplace model has been commonly adopted with 2-3 ‘mandatory' office days, and the balance of work executed remotely.

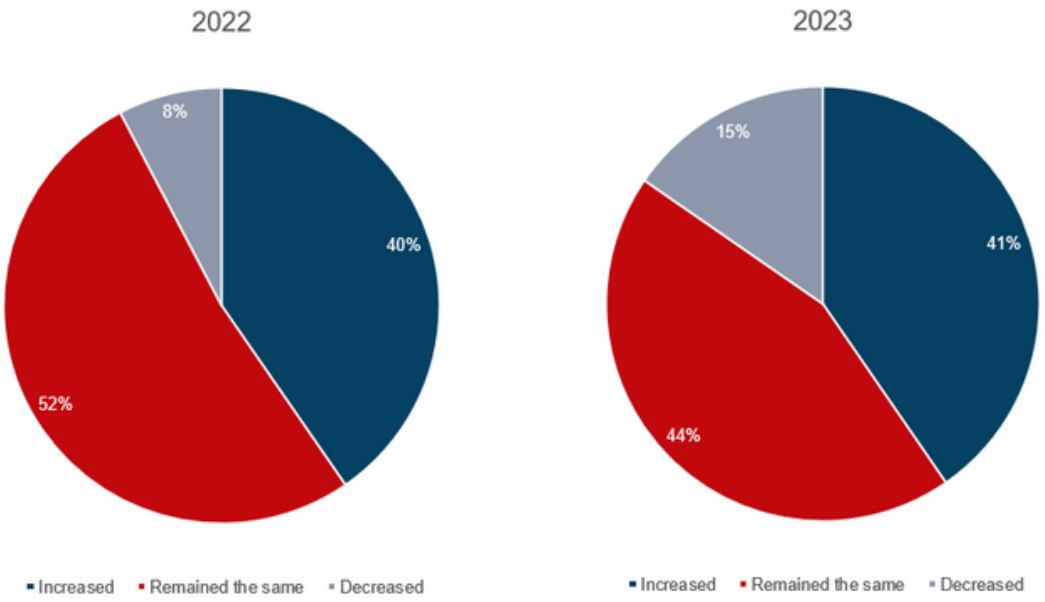
Security and Office Infrastructure

Some organizations leveraged the pandemic pause as an opportunity to rip and replace security equipment while office space stood empty. Security teams were also pulled into the overall conversation regarding the organization’s office/real estate footprint in response to evolving workplace models. Furthermore, team responsibilities have expanded to include other business processes like visitor management, asset management and contractor management.

Budgets and Finances

The Security Budget

The vast majority (84%) of security practitioners expect their budgets to be maintained or increased in 2023. Though, for those who have managed flat or decreased budgets in 2022, the outlook for 2023 is slightly more negative.



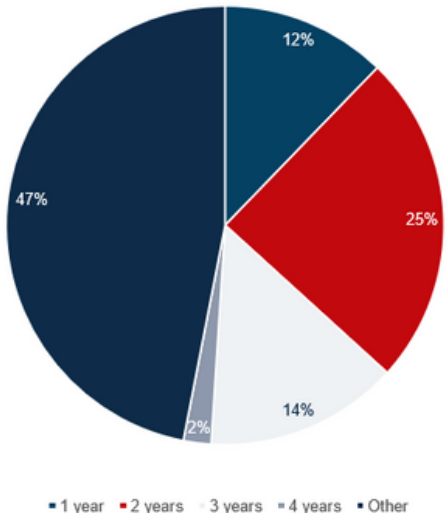
Investments

The top 3 investments for both 2022 and 2023 are:

1. Access control upgrades
2. Staffing and security guards
3. System maintenance

ROI

ROI expectations vary by organization. Respondents to the survey noted what they perceived to be acceptable payback in the context of their organization.



That said, despite their understanding of organizational expectations, security leaders have a difficult time quantifying their return on investment for physical security and instead leverage incident reporting and management figures for cost justification. Indeed, 47% of respondents noted that they have no real ROI measurement in place for security equipment/initiatives or understanding to support implementation.

Cost Reduction

Survey respondents cited numerous cost reduction measures including:

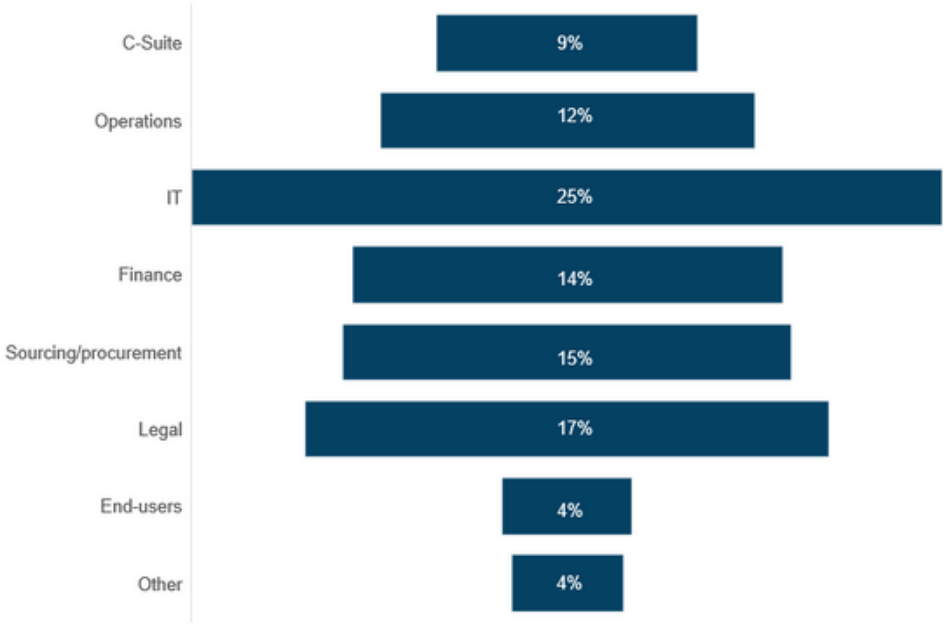
- Increasing in-house labor, to reduce vendor costs
- Decreasing next year's budgets
- Looking at technologies to replace manpower
- Leveraging unified platform and standardization across the board
- Planning exercises to see what is coming
- Negotiating with vendors to reduce costs for hardware/software, maintenance and services

Insight: Nearly half of the organizations that told us they have a cost reduction effort in place were unable to describe what specific goals need to be achieved, indicating a greater need for organizational communication.

Sourcing and procurement

According to respondents, when it comes to sourcing and procurement:

- More than half don't control the entire security budget and are dependent on other business units to fund physical security projects and initiatives.
- Equipment/technology approvals are contingent on IT involvement 78% of the time and c-level executives 31% of the time.



Insight: A total cost of ownership (TCO) financial model helps security functions understand the total cost of their program including things like fully burdened internal/external labor, hardware/software costs and ongoing maintenance costs, among others. This financial information is critical to establish return on investment (ROI) and/or cost benefit analysis (CBA) when seeking funding for key initiatives and ongoing program support.

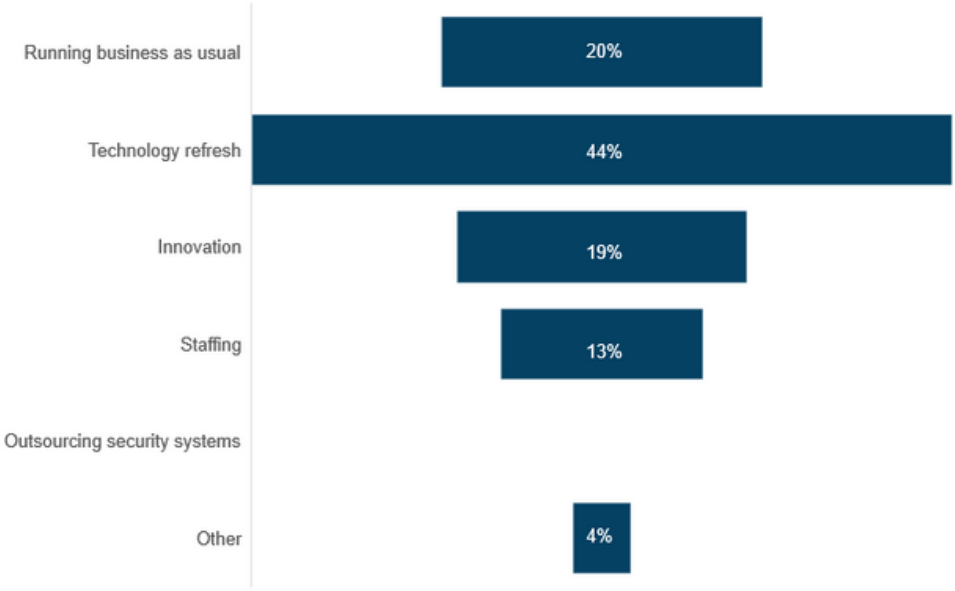
Strategy and Innovation

Security Resources

While some security teams anticipate a slight increase in their headcount for 2023, the majority (54%) expect resources to be unchanged mainly due to hiring challenges and finding the right talent. That said, 48% currently have open positions which they aspire to fill.

Overall Strategy

When asked about their major focus for 2023, respondents noted that their teams would be focused on:



Longer-term, 44% asserted that they don't have a strategy fully in place. Those that did note long-term plans seemed to be more focused on tactics than actual strategy. And very few respondents addressed 3-5 year planning in detail.

Innovation Drivers

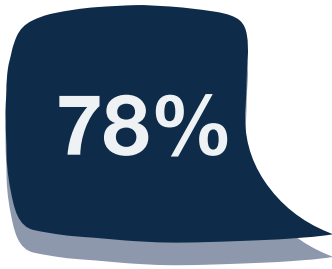
The need for increased operational efficiencies emerged as the primary driver for cross-industry innovation in this survey. Indeed, 44% cited their innovation focus as utilizing data and technologies to reduce man-power and increasing workflows and processes.

Successful initiatives were overwhelmingly facilitated by collaboration with IT and Operations.

That said, very few respondents were able to describe how they measure success for innovation projects. Delivery within time and budget was commonly noted but this is a process driven measurement, as opposed to a true assessment of outcome.

Insight: There is a huge opportunity for physical security leaders to develop KPIs and measurement for success to better lead innovation in collaboration with other departments like IT, Operations and Marketing.

Innovation Inhibitors



The most significant innovation inhibitor for security leaders is financial. Indeed, 78% of survey respondents told us they have no innovation budget available, therefore any necessary funds need to be pulled from other initiatives and/or departments.

Digital Transformation

IT is leading Digital Transformation initiatives according to 56% of respondents, whereas only 10% of participating organizations have a separate Digital Transformation team in place. And interestingly, the remaining 34% have no idea if there is a Digital Transformation strategy in place, never mind who is leading the effort.

Most importantly, 36% of security teams work in collaboration with IT on DT projects but more than half (55%) are not involved in DT initiatives at all.

Insight: With available physical security technologies like AI, ML, Mobile credentialing, and autonomous solutions, security leaders should be involved if not leading Digital Transformation activities for their organizations.

The Big Issues in Security

Cloud Strategy

Moving to the cloud has ramifications for security, yet 78% of security teams surveyed are currently uninvolved in the corporate cloud strategy! Instead, 81% noted IT as the 'owner' of their organization's cloud strategy. And surprisingly 19% of respondents did not know who owned the strategy and 30% didn't know what was driving it. This is in the context of an uptick in cloud adoption. Almost all organizations (98%) surveyed have a cloud strategy in place and more than a quarter (27%) of respondents indicated that their organization has a 'cloud first' mentality.

What is driving cloud adoption? Most say cost, yet measurement of cost savings has been elusive for many. Therefore, pre-research and comprehensive cost saving analyses are recommended before transitioning fully to the cloud. This includes assessing any perceived risks. Survey respondents noted that their organization's number 1 reason for not moving to the cloud is security concerns (35%), followed by network readiness (22%). Many security leaders believe their (IT) infrastructures are not (cyber) ready to go cloud native.

Insight: More than half (51%) of security respondents don't fully understand their organization's current cloud strategy. This is particularly alarming given the intensive data collection associated with video. Given available technologies and solutions, cloud strategy/management should be a top priority for security leaders, and they should be a more significant player in the overall process. And while IT should enable and support deployment of the cloud strategy, they should not own it. Ultimate ownership for cloud strategy is topline and should therefore fall on the shoulders of the board of directors and executive leadership.

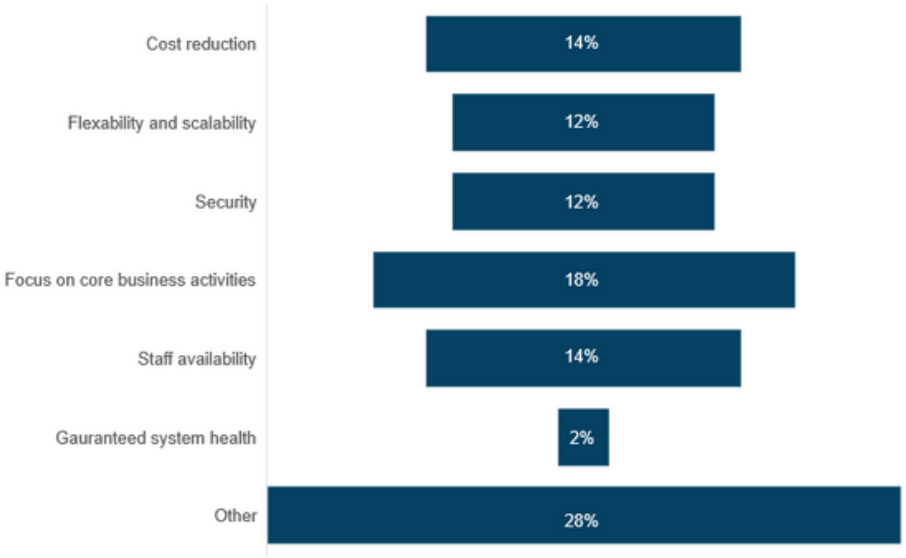
Cyber Security

Only 4% of physical security teams are leading cyber security initiatives for their respective organizations. Another 18% are teaming up with IT. **And a whopping 63% of respondents noted that they are not involved at all in corporate cyber security initiatives and strategy!**

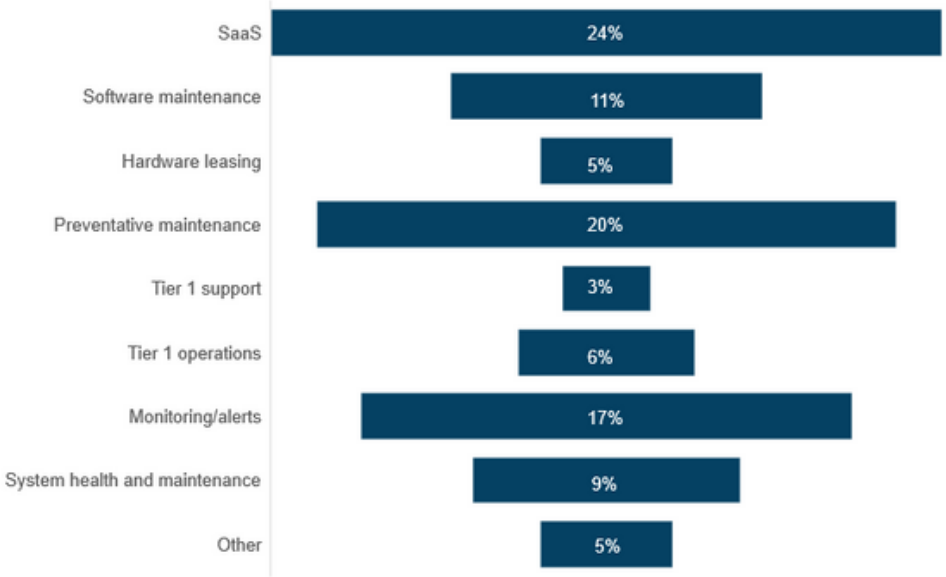
Insight: Cyber security is considered one of the biggest risks for the organization. Outside actors are making news with attacks on our national infrastructure. Internal expertise is critical for navigating threats and managing vulnerabilities can be overwhelming. The lack of resources dedicated to fully securing organizational assets and data is a problem.

Outsourcing

In order to make up for the lack of resources and overworked staff, many organizations are looking to outsource their physical security department. This is driven by a number of factors:



What is most commonly outsourced? Those respondents that planned to subcontract in the next 12 months broke things out as follows:



Survey Conclusions

The days where the physical security team was simply viewed as a reactive cost-center are long gone thanks in part to the digital revolution. With a transformed threat landscape and the impact of cloud computing, security now requires reassessment in partnership with IT. Artificial Intelligence and Machine Learning specifically demand attention as they are driving new approaches to the management of security breaches and incidents. Data outcomes can be leveraged for proactive detection and risk mitigation, versus reactive response. This evolution has expanded the responsibilities of physical security leaders who now must both provide a safe work environment and spearhead new ways to deliver data intelligence to support business outcomes. Many organizations are therefore exploring ways to outsource some of their business support functions, including physical security, to alleviate pressures on staff and allow them to focus on core business activities.

Success begins by building a solid long term physical security strategy that echoes the organization's mission and culture, whilst demonstrating the business value of physical security. A total-cost-of-operations model (TCO) combined with a ROI-centric strategy should allow the security department to provide the business with a better understanding of its costs and added value to the business. Building strong relationships with other departments like IT, operation and facilities are key to fully demonstrating how physical security can bring value to the table.

Many leaders told us they have had difficulties showing ROI for physical security technology investments. That said, alignment with organizational goals and providing the right data to internal stakeholders and end-users could surely boost their success in securing funding. The burden is on them to establish the value of physical security by demonstrating how data can be applied to create operational efficiencies, cost savings and increased colleague/customer satisfaction, whilst they maintain a safe and secure workplace.

Lastly, cyber security is seen as one of the biggest threats to your organization, however many physical security leaders are not involved in the organization's cyber strategies and initiatives. It is imperative that physical security teams seek out opportunities for alignment with IT so that they can increase engagement. There is a huge opportunity for physical security teams to show how video, access control and surveillance data can support all business processes and growth. This shift will empower security departments to become a true business enabler.