IT Key Metrics Data 2023: IT Security Measures — Analysis

Published 8 December 2022 - ID G00779671 - 11 min read

By Analyst(s): Eric Stegman, Jamie Guevara, Nick Michelogiannakis, Shaivya Kaushal

Initiatives: Technology Finance, Risk and Value Management; Security Operations

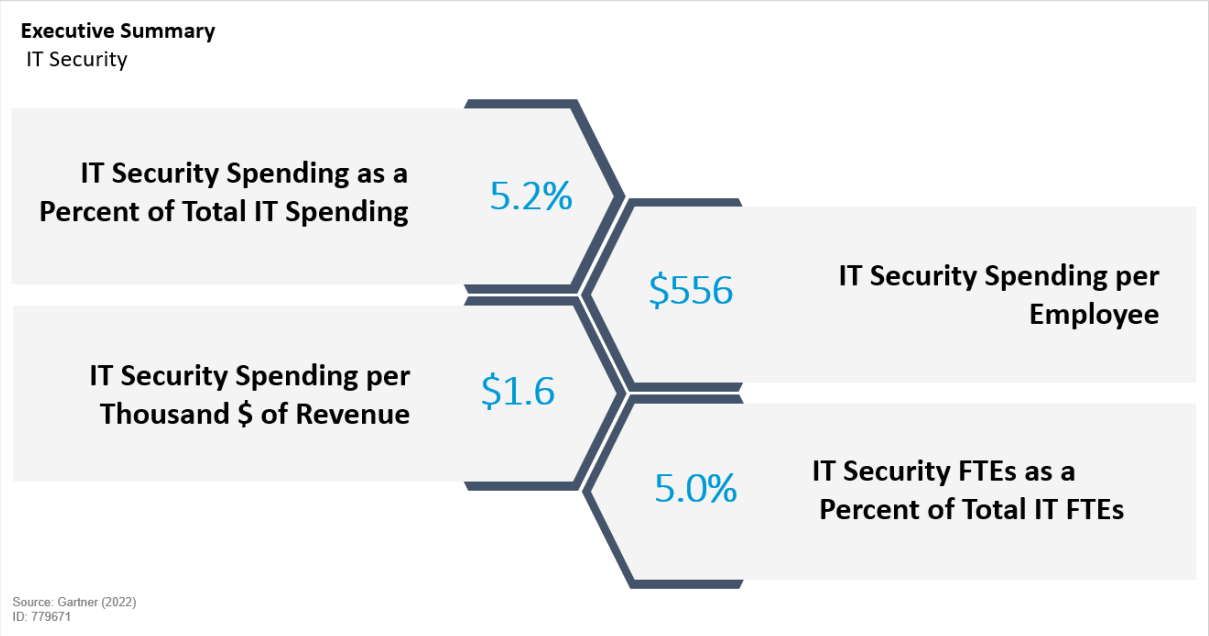
This research contains high-level IT Security cost efficiency and staff productivity benchmarks which should be used as part of a perennial cost and value optimization program. The published information derives from data collected throughout 2022 from a global audience of CIOs and IT leaders. Key cost and support distributions as well as metrics based on industry segments are also included.

Overview

The aim of this report is to help IT organizations assess their IT Security spending and staffing efficiency and suitability at a high level. IT Security spending and staffing are distributed in operation, indicating what types of investments the enterprise is making. Further distribution of operational infrastructure security spending by task helps to outline technology-based spending allocations.

Spending is also broken down to the four Gartner asset classes (Personnel, Hardware, Software & External Services) to allow for more granularity, better interpretation and easier identification of the key cost/gap drivers.

Figure 1: Executive Summary for IT Security



Key Findings

- For 2022, median IT security and risk management investment accounts for 5.2% of total IT spending up from 5.0% last year as mandates for risk reduction were at least as important as revenue generation and cost reduction.
- The percentage of IT Security Spending on traditional reactive functions IT Infrastructure Operational Security (Firewalls/anti-virus) continued to fall relative to more proactive functions such as vulnerability and analytics.
- The 2022 median IT security FTEs as a percent of Total IT FTEs is 5.0% up from 4.7% last year, and has driven organizations to take steps to optimize personnel spending in a tight job market.

Recommendations

- Leverage the available published content to evaluate your organization or receive a report tailored to your organization by completing the Gartner IT Budget Tool
- Refer to the available supporting documentation such as the "IT Key Metrics Data 2023: IT Security Measures — Framework Definitions" to better understand the consensus model and the methodology behind the metrics.
- Follow the Practitioners Guide to best prepare your data for comparison.
- Schedule an inquiry to review your results or address alignment questions or to review your results and gain valuable insight based on your submission.

Clients improve business performance by benchmarking their spending and best practices against Gartner's IT performance repository, the largest in the industry, drawing on over 5,000 IT benchmarks a year. The scope of this high-level IT Security Report includes IT Operational Infrastructure Security, Vulnerability and Security Analytics, Application Security, and Governance, Risk, and Compliance.

This research provides an overview of the Gartner Benchmark Analytics consensus model and high-level summary data from our global cost benchmark observations. The published information only represents a subset of the metrics and prescriptive analysis capability available through Gartner Benchmark Analytics.

The metrics explored include cost efficiency and support productivity metrics in terms of total employee and revenue for the IT security environment. These medians provided do not account for individual variations of service quality, complexity or demand which may be justified by specific business needs. The data here should be used as reference points to put any individual organizations spending in perspective and not as prescriptive targets.

For all of the efficiency and productivity metrics in this document, the interquartile range represents the 25th to 75th percentile and designates the span where half the data falls. The range includes the 10th to 90th percentile. There are organizations with unique requirements that extend far beyond the upper bounds.

Determining the right level of security investment involves much more than “matching” a database median. Factors such as level of risk, past investment, and organizational culture also play important roles. These metrics should be considered within the context of the overall information security and risk management strategy i.e., as the technology environment plays a lesser or greater role in mission-critical business processes, so will the need to mitigate risk by maintaining and managing a secure technology environment.

IT Security Spending as a Percent of Total IT Spending

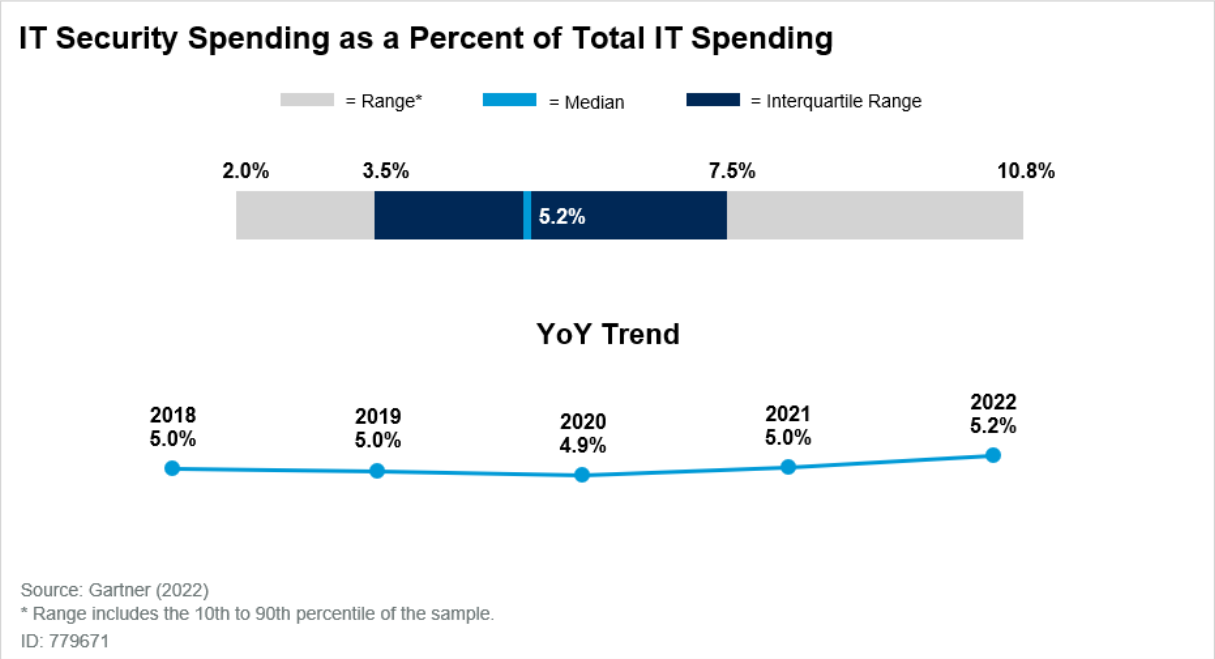
IT security spending as a percent of total IT spending (Figure 2 & 3) is helpful in understanding the relative level of investment to support the security of the total IT environment from a total IT portfolio perspective.

As the workload factor, here “IT spending”, organizations with a higher percentage have more IT security spending relative to their level of total IT spending. Subsequently, two organizations may spend the same nominal amount on IT Security, but one of them will be higher on this metric if they have a lower level of total IT spending.

Here we see that some industries with high IT Spending relative to workload factors as noted in “IT Key Metrics Data 2023: Industry Measures — Executive Summary” such as Software Publishing and Internet Services and Banking and Financial Services, are also high on this metric. While Education has a high level of overall IT spending it comes in lower on this metric.

Companies tend to strive for cost optimization by being careful about spending on functions like IT Security that don’t drive revenue or reduce costs in other parts of the business. The increase in this metric over the past two years at the cross industry level is due to the fact that companies are willing to invest in IT Security because it reduces risk.

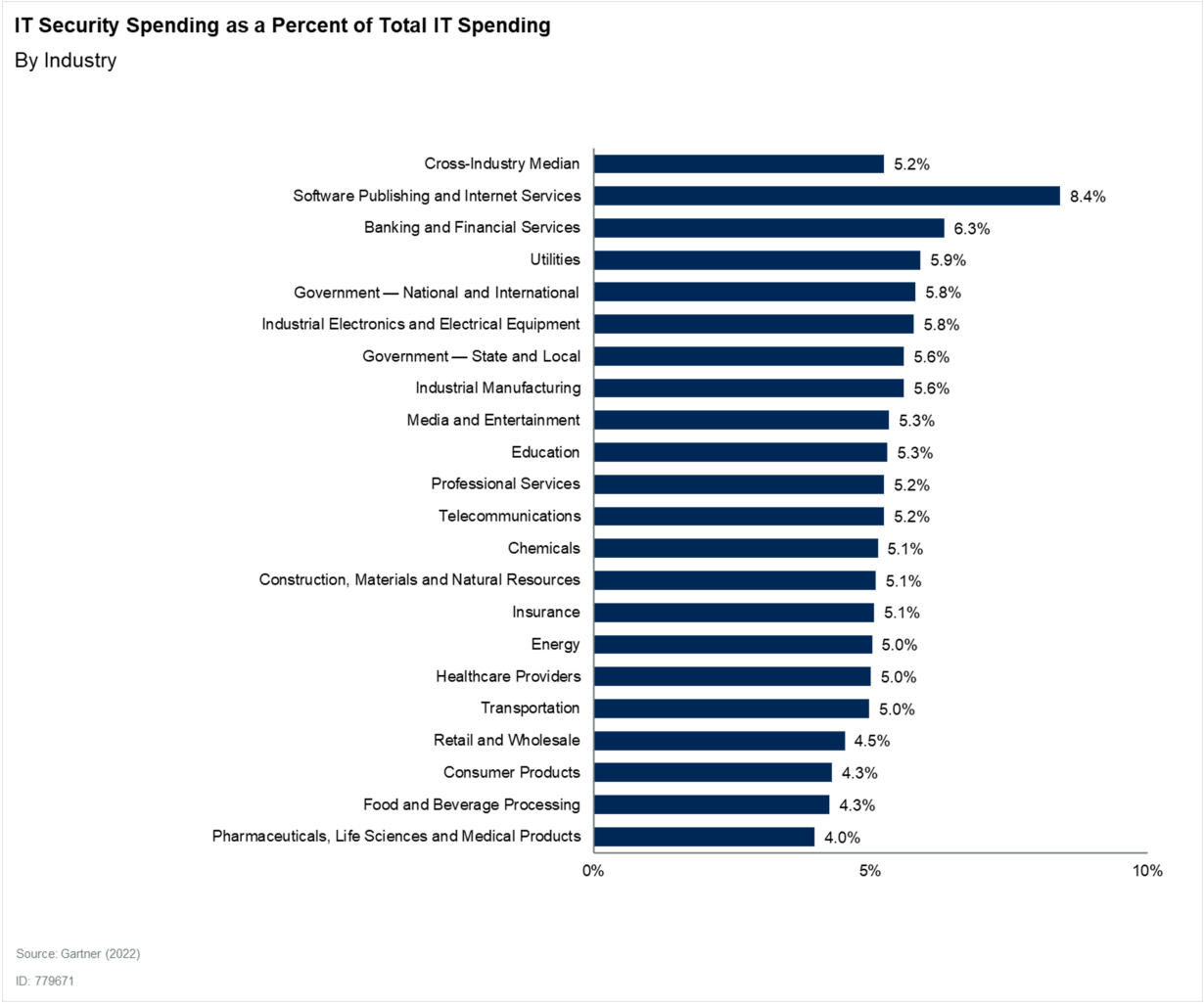
Figure 2: IT Security Spending as a Percent of Total IT Spending



Source: Gartner (2022)
* Range includes the 10th to 90th percentile of the sample.
ID: 779671

Gartner

Figure 3: IT Security Spending as a Percent of Total IT Spending, by Industry



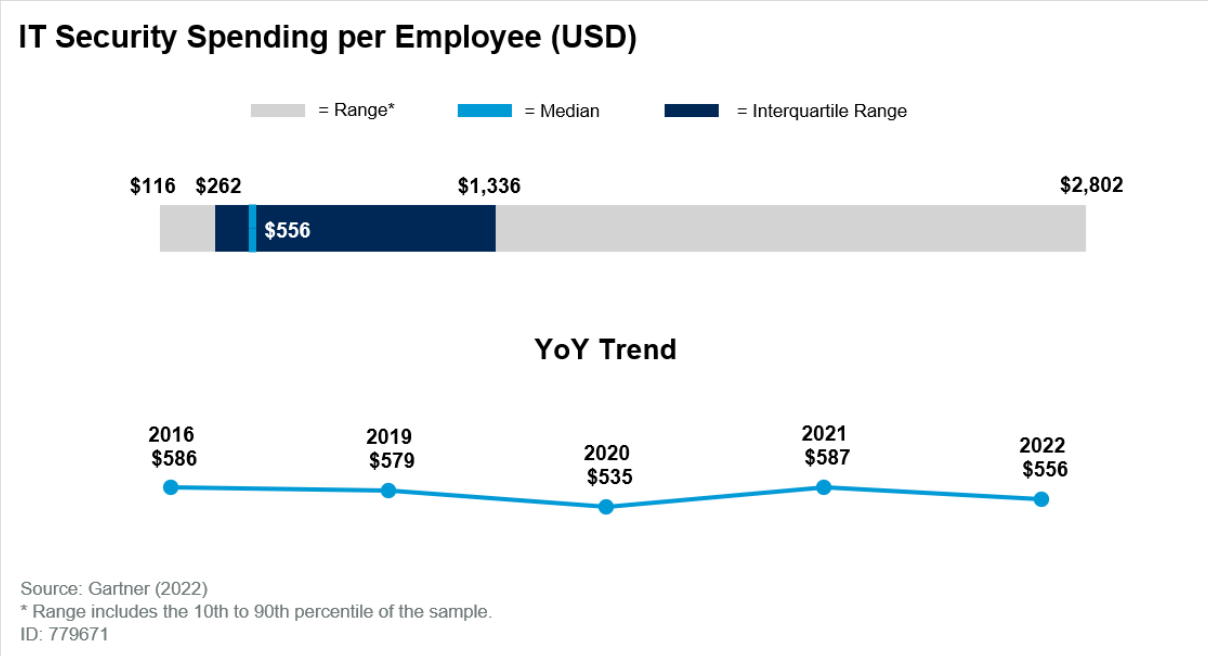
IT Security Spending per Employee

IT security spending per employee (Figure 4 & 5) is another indicator of total security investment.

Using this denominator provides a more stable baseline since the number of employees tend to vary less year to year than IT spending does. This metric is dependent on how “people intensive” the enterprise is. It is useful to understand Enterprise IT Spending per Employee relative to peers in conjunction with this metric.

This metric declined slightly from our report last year. This is unusual given increased IT Security spending but may be due to companies hiring more non-IT staff.

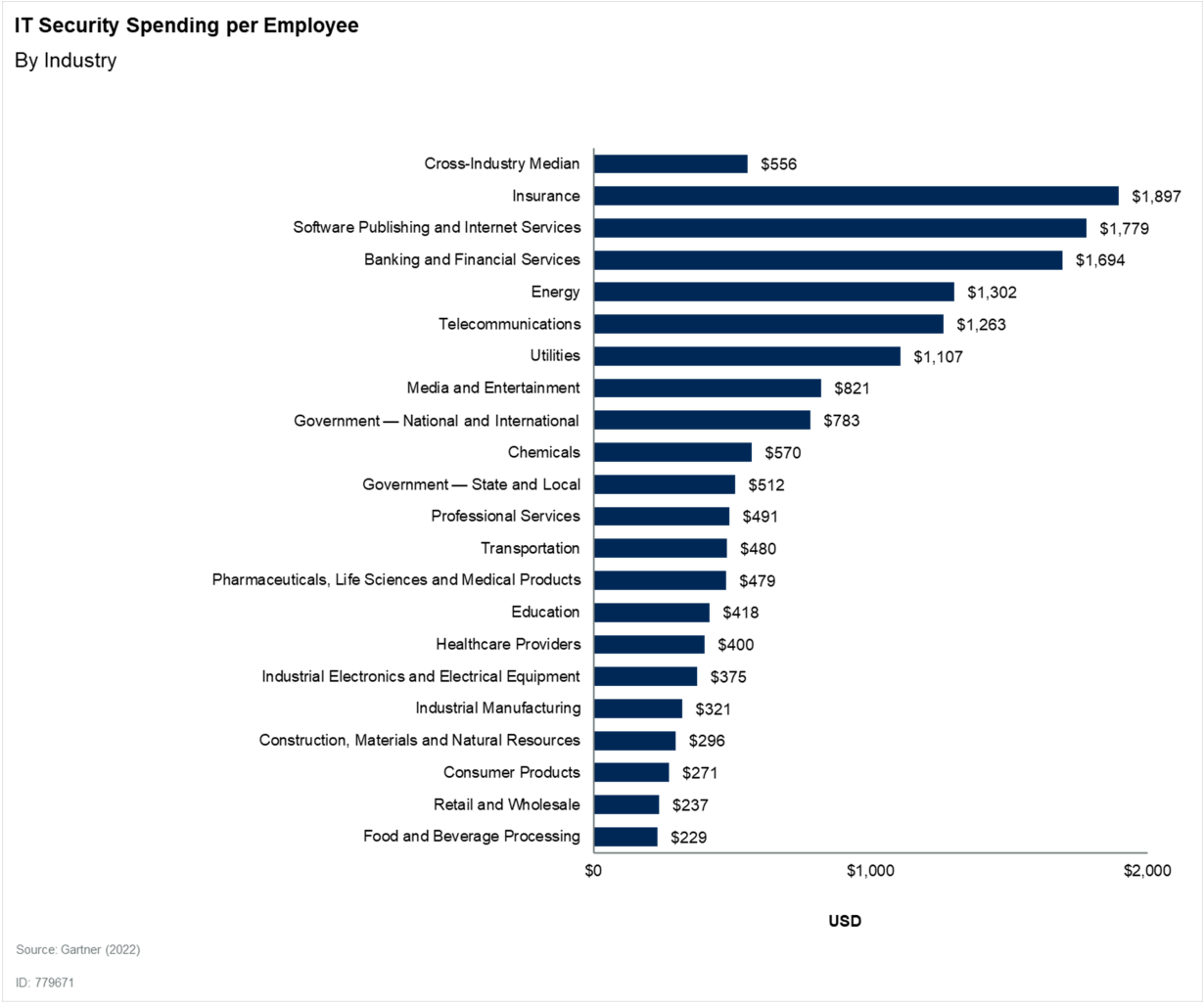
Figure 4: IT Security Spending per Employee (USD)



Source: Gartner (2022)
* Range includes the 10th to 90th percentile of the sample.
ID: 779671

Gartner

Figure 5: IT Security Spending per Employee, by Industry

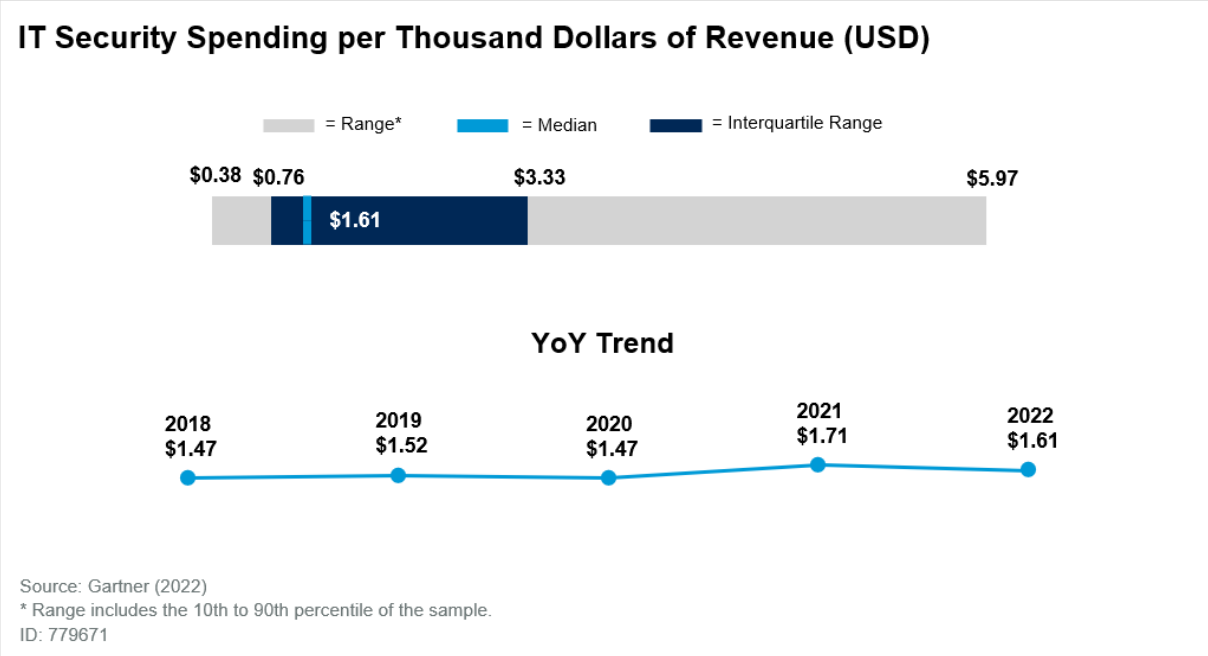


IT Security Spending per Thousand Dollars of Revenue

IT security spending per thousand dollars of revenue (Figure 6 & 7) is calculated as IT security spending/(revenue/1000). The denominator is expressed in thousands to prevent the value of the metric from being a very small number. The metric is just a ratio so while we show “Dollars” it makes sense in any currency e.g., Euros, Pounds etc.

It reflects the investment in security relative to the size of the business from a financial perspective. This additional view can supplement the IT security spending per employee metric when staffing strategies vary between enterprises.

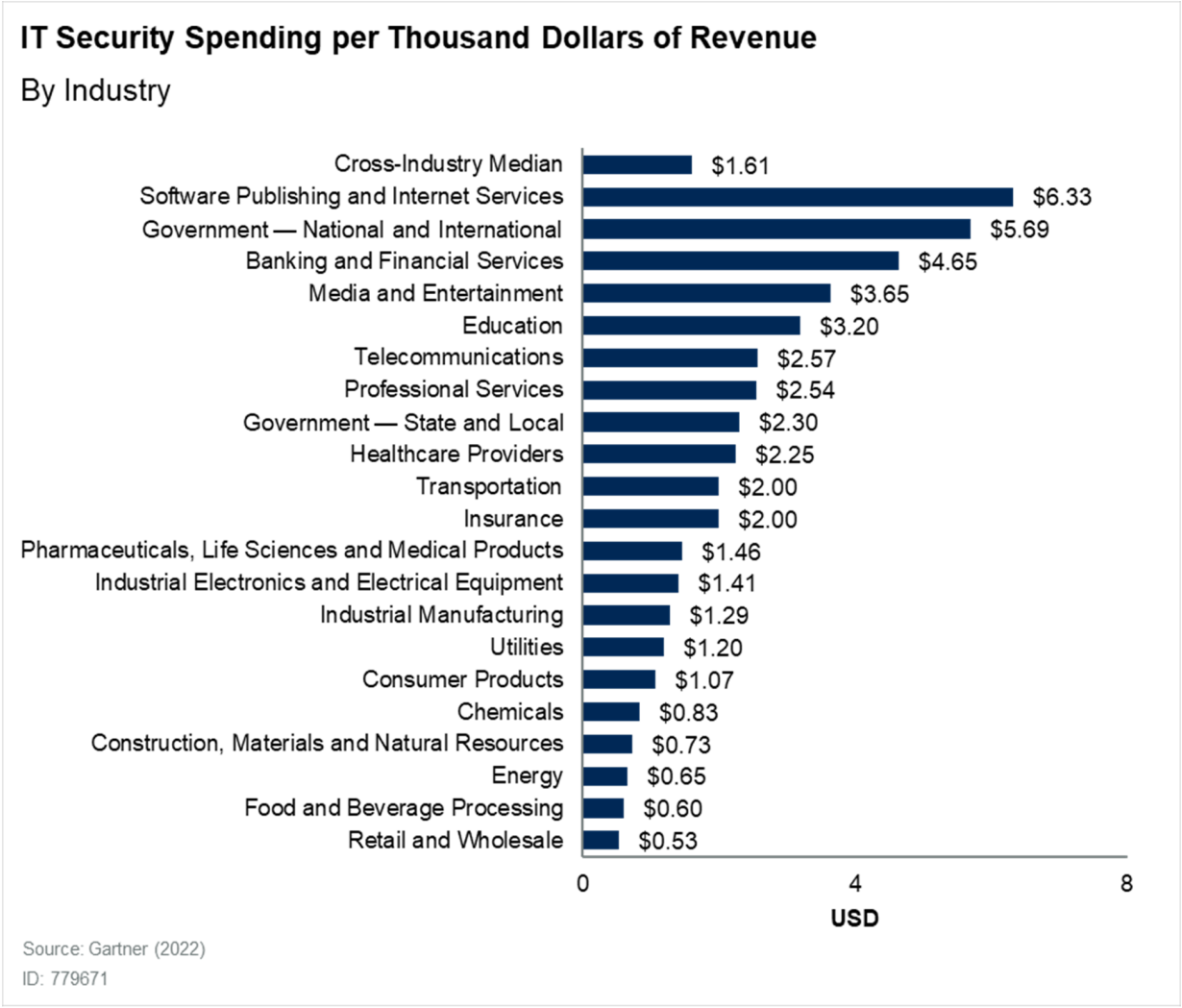
Figure 6: IT Security Spending per Thousand Dollars of Revenue



Source: Gartner (2022)
* Range includes the 10th to 90th percentile of the sample.
ID: 779671

Gartner

Figure 7: IT Security Spending per Thousand Dollars of Revenue, by Industry



IT Security Spending by Operation

IT security spending distribution by operation (Figure 8 & 9) is important as it indicates what types of investments the enterprise is making.

Operational infrastructure security spending is focused on protecting the network, hosts and data and ensuring secure access to systems for authorized users. However, most enterprises recognize that they cannot “keep the bad guys out” by automated preventative measures alone. A mature set of information security measures combines effective “detect” and “respond/mitigate” tools with “prevent” services, and also proactive “predict” services to intercept potential cyber-attacks and threat actors before they even occur.

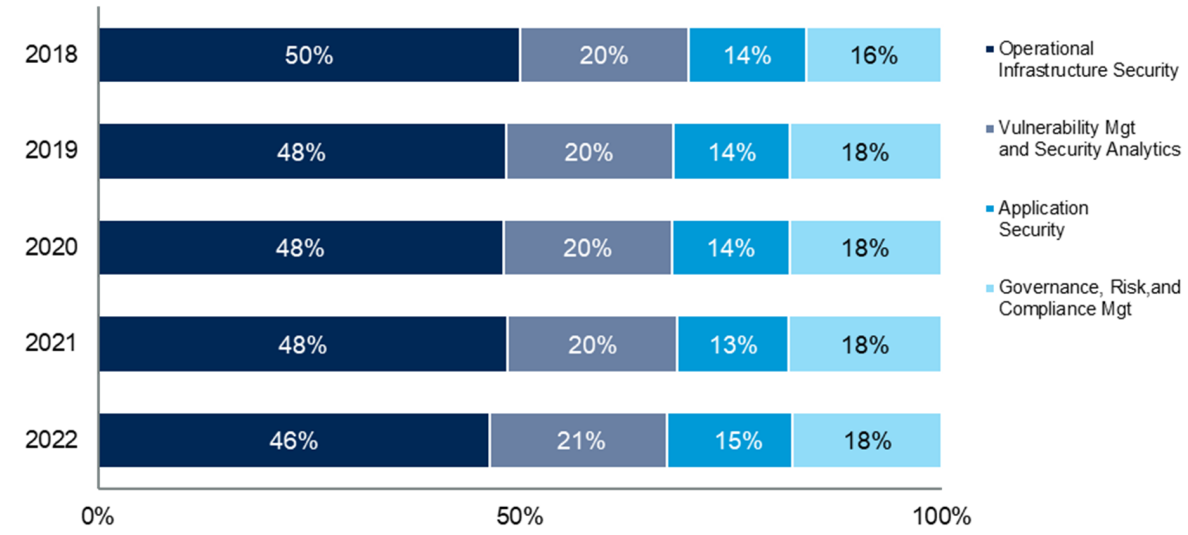
Vulnerability management and security analytics are focused on more mature and proactive capabilities and on minimizing the impact of any breaches once they have occurred.

Application security spending deals with how the application was designed and developed, how it is operated, and how the application and its supporting elements (network, OS, database and so on) are configured and deployed. It makes sure all of this is done in a secure manner. It adds an extra level of security at the application layer of the OSI model. It is helpful in protecting the business when the requirements dictate that less trusted sources must be allowed through the infrastructure protection.

Governance, risk, and compliance management spending focuses on how the organization deals with its unique set of risks. It creates strategies, policies, standards and awareness that underpin security services. It ensures that risk is managed openly and effectively, that legal and regulatory compliance is ensured, and that information security is embedded throughout the enterprise. This can be seen as an investment in the process.

Over the past few years we have seen a slight reduction in the more traditional reactive Operational Infrastructure functions and toward the more proactive functions in the other categories in the model.

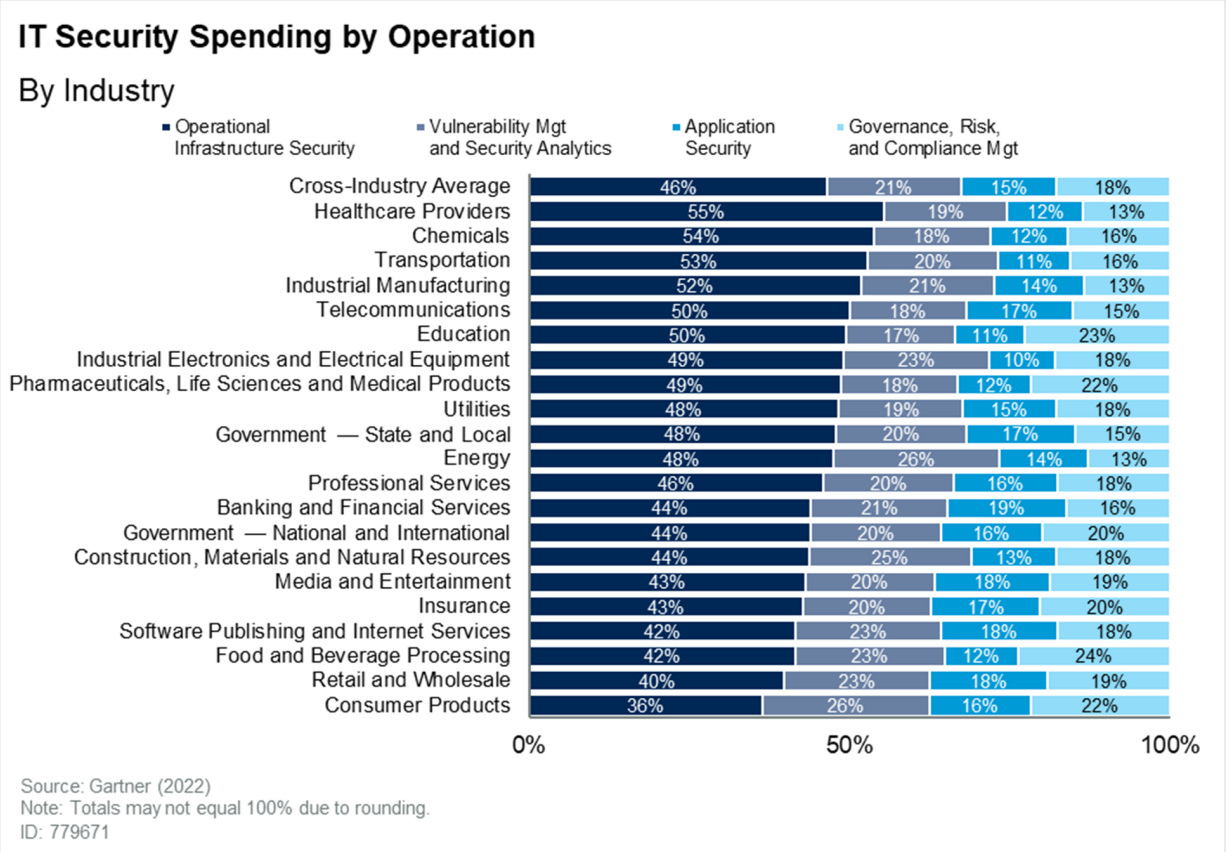
Figure 8: IT Security Spending by Operation



Source: Gartner (2022)
Note: Totals may not equal 100% due to rounding.
ID: 779671

Gartner

Figure 9: IT Security Spending by Operation, by Industry

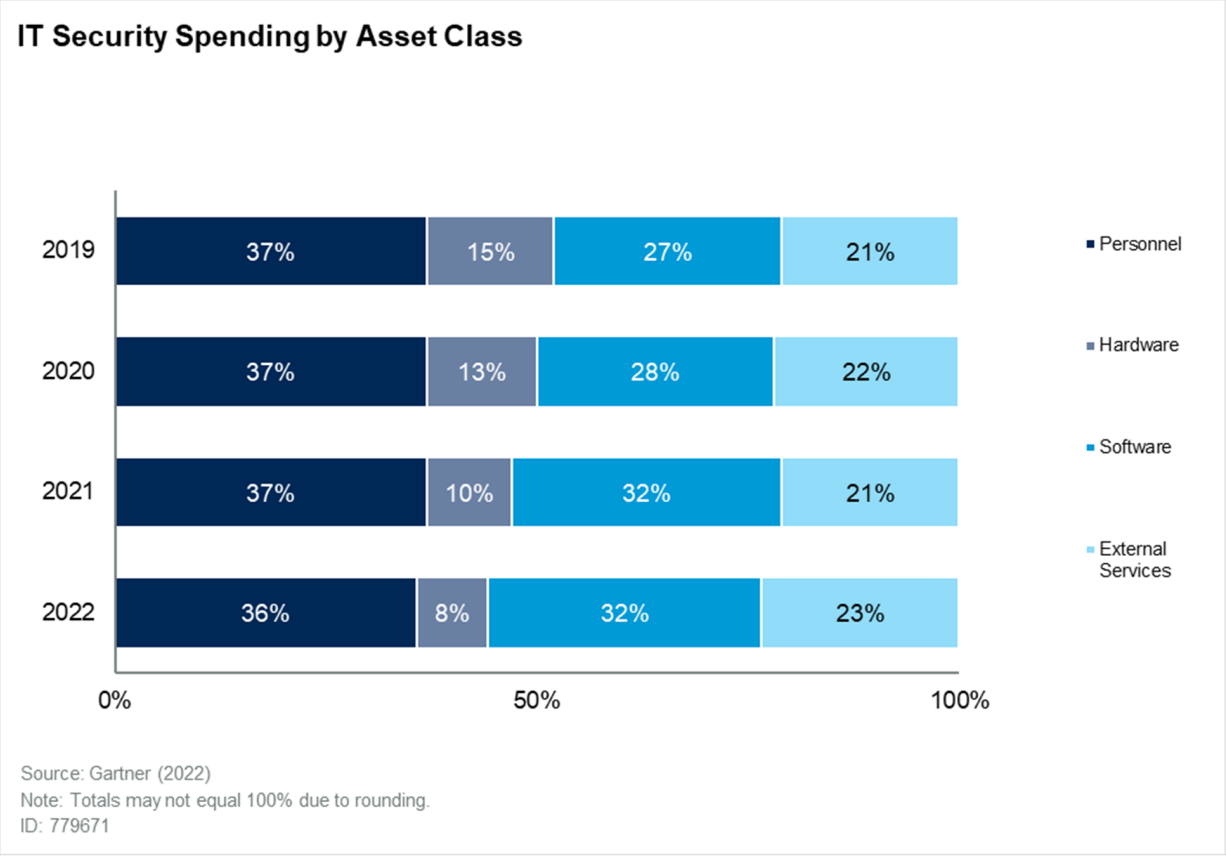


IT Security Spending Distribution by Asset Class

The distribution of IT security spending by asset class (Figure 10 & 11) provides an understanding of how investments are dispersed within the environment. This distribution helps to outline non-personnel versus personnel related cost allocations.

As we have three consistent years of data here, we see a shift away from hardware and towards software. This makes sense as the price of hardware drops and spending on items like firewalls associated with reactive security makes way for software that is more associated with a proactive approach. The use of software can also have an effect of reducing labor requirements in a tight job market.

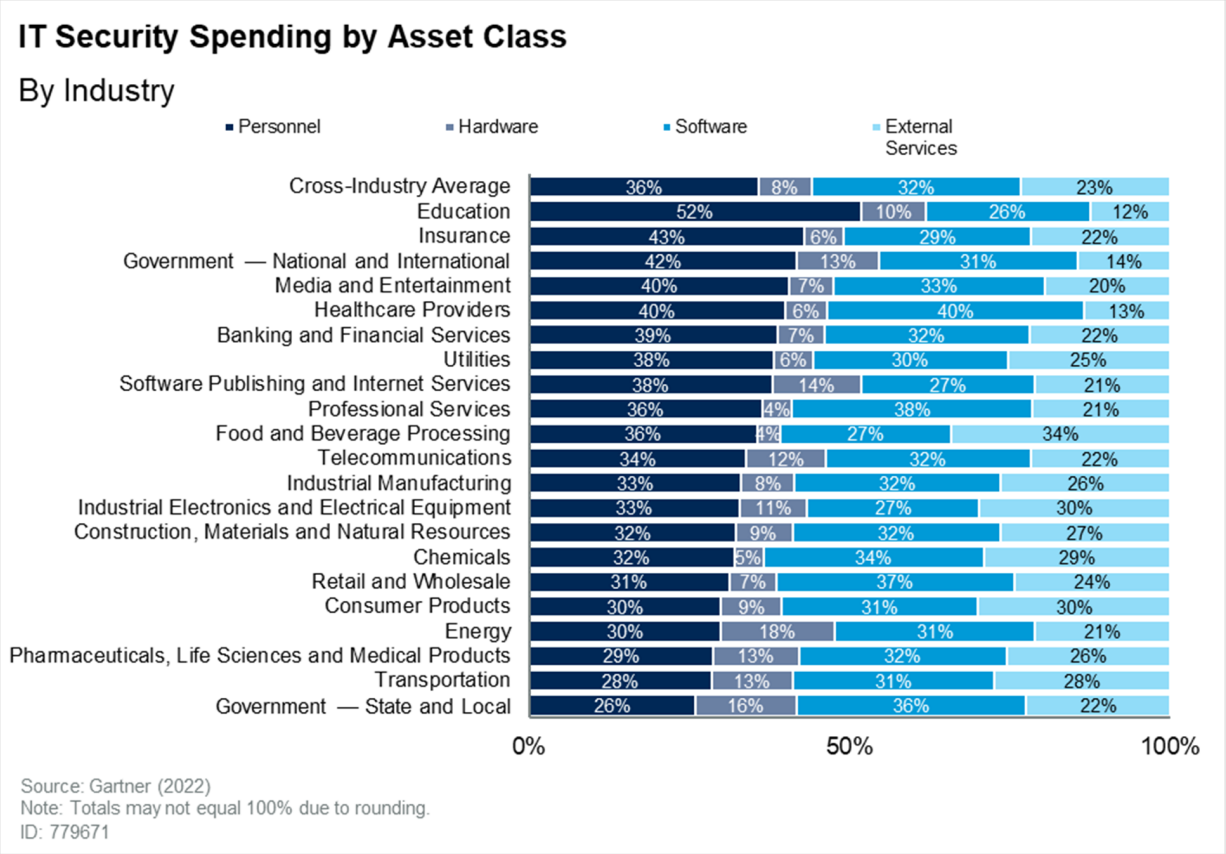
Figure 10: Distribution of IT Security Spending by Asset Class



Source: Gartner (2022)
Note: Totals may not equal 100% due to rounding.
ID: 779671

Gartner

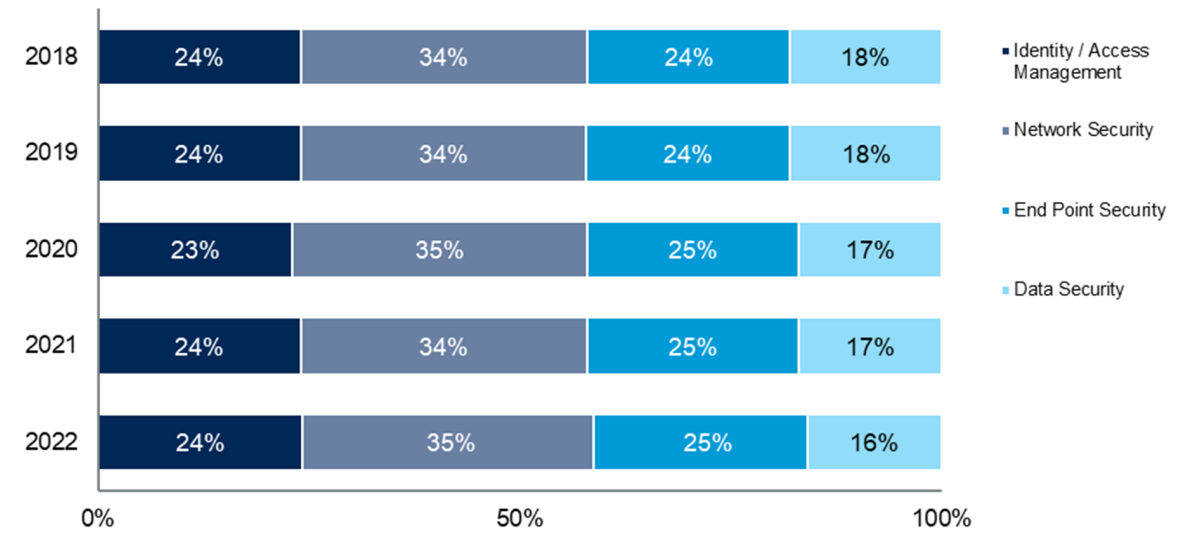
Figure 11: Distribution of IT Security Spending by Asset Class, by Industry



Operational Infrastructure Security Spending Distribution by Task

The distribution of operational infrastructure security spending by task (Figure 12 & 13) provides an understanding of how security investments are dispersed across the technology environments. This distribution helps to outline technology-based spending allocations.

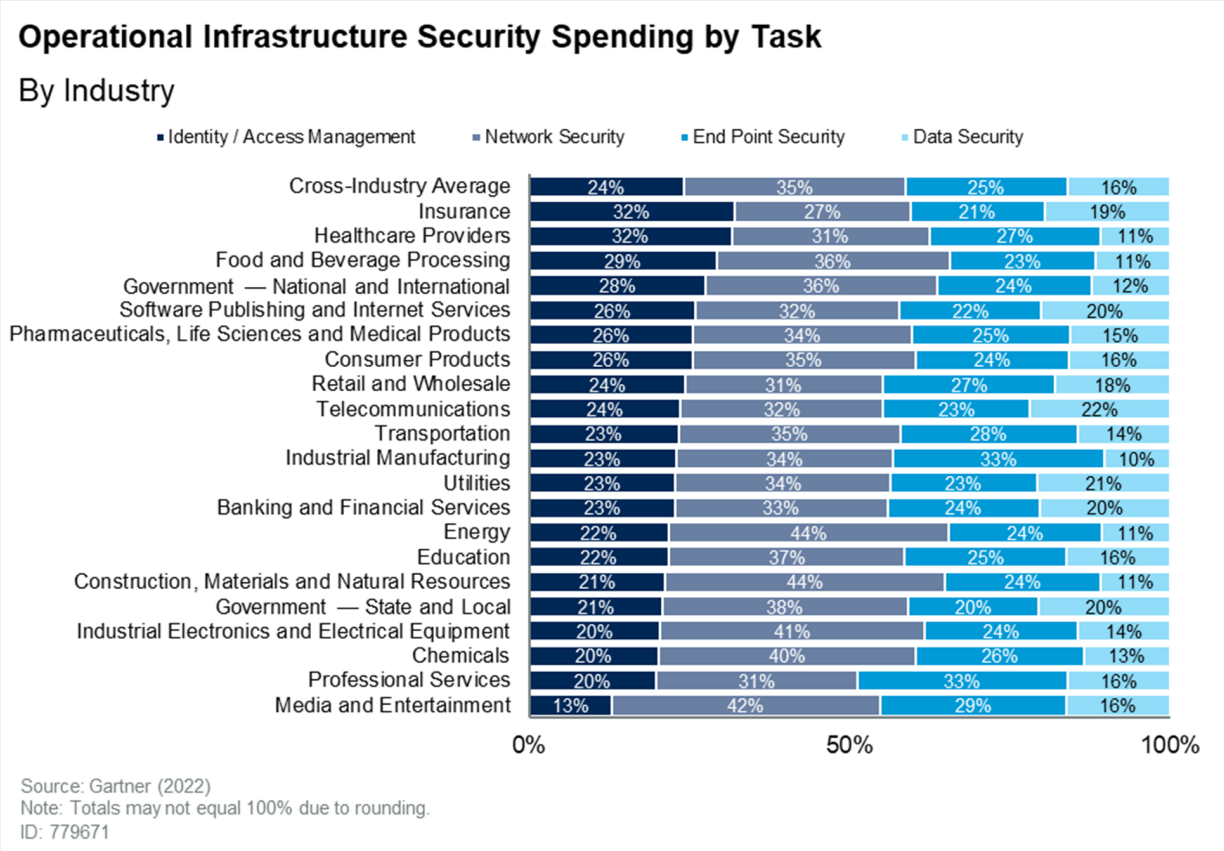
Figure 12: Distribution of Operational Infrastructure Security Spending by Task



Source: Gartner (2022)
Note: Totals may not equal 100% due to rounding.
ID: 779671

Gartner

Figure 13: Distribution of Operational Infrastructure Security Spending by Task, by Industry



Gartner

IT Security FTEs as a Percent of Total IT FTEs

IT security FTEs as percent of total IT FTEs (Figure 14 & 15) is a measure of IT security support intensity from a human capital perspective.

IT security personnel includes in-house and contract full-time equivalents supporting the following IT security operations: Operational infrastructure, vulnerability management and security analytics, application security, and governance, risk, and compliance management.

Understanding the relative level of security support dedicated to an IT environment can also assist in identifying whether staff size is appropriate. This should be considered within the context of the overall sourcing strategy and future state objectives. Variables to consider in tandem with this metric include: IT staffing distribution: contract versus insourced FTEs, the percentage of the environment outsourced (supported by a third-party), as well as the evolving business requirements.

This metric has increased over the past several years even as the percent of spending on personnel has been relatively flat. It's difficult to tell exactly why this is happening, but anecdotally we have seen some clients move security tasks to other IT teams such as infrastructure. We have also seen internal training programs to reduce the need to tap a difficult hiring market.

Figure 14: IT Security FTEs as a Percent of Total IT FTEs

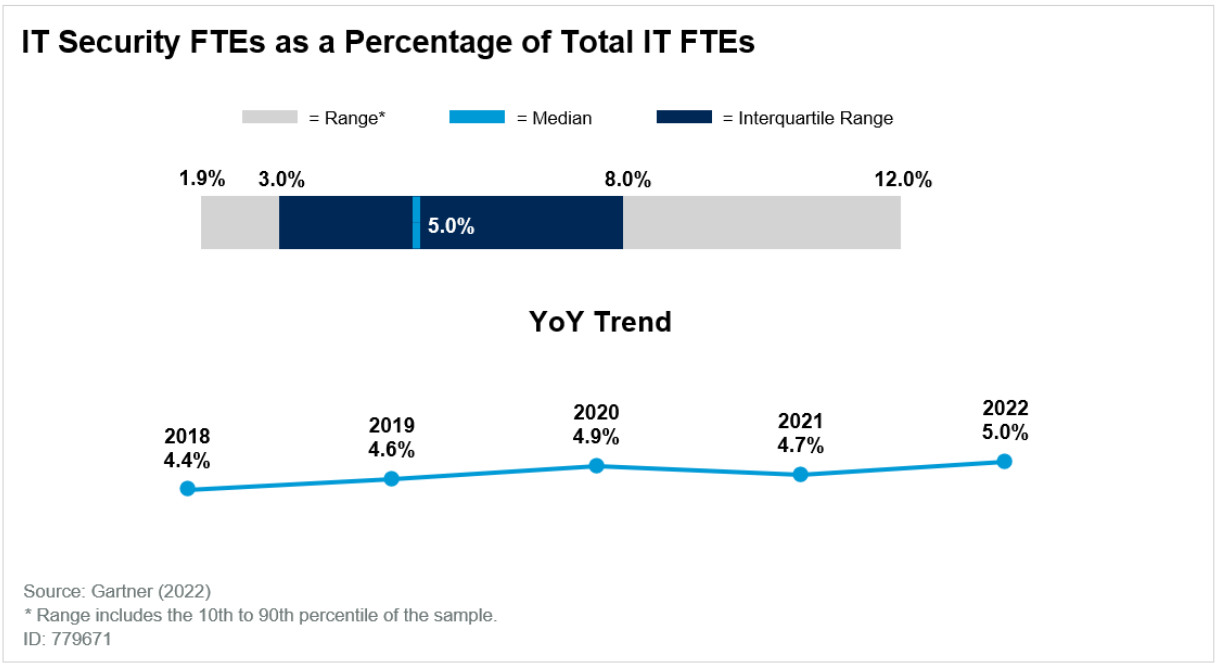
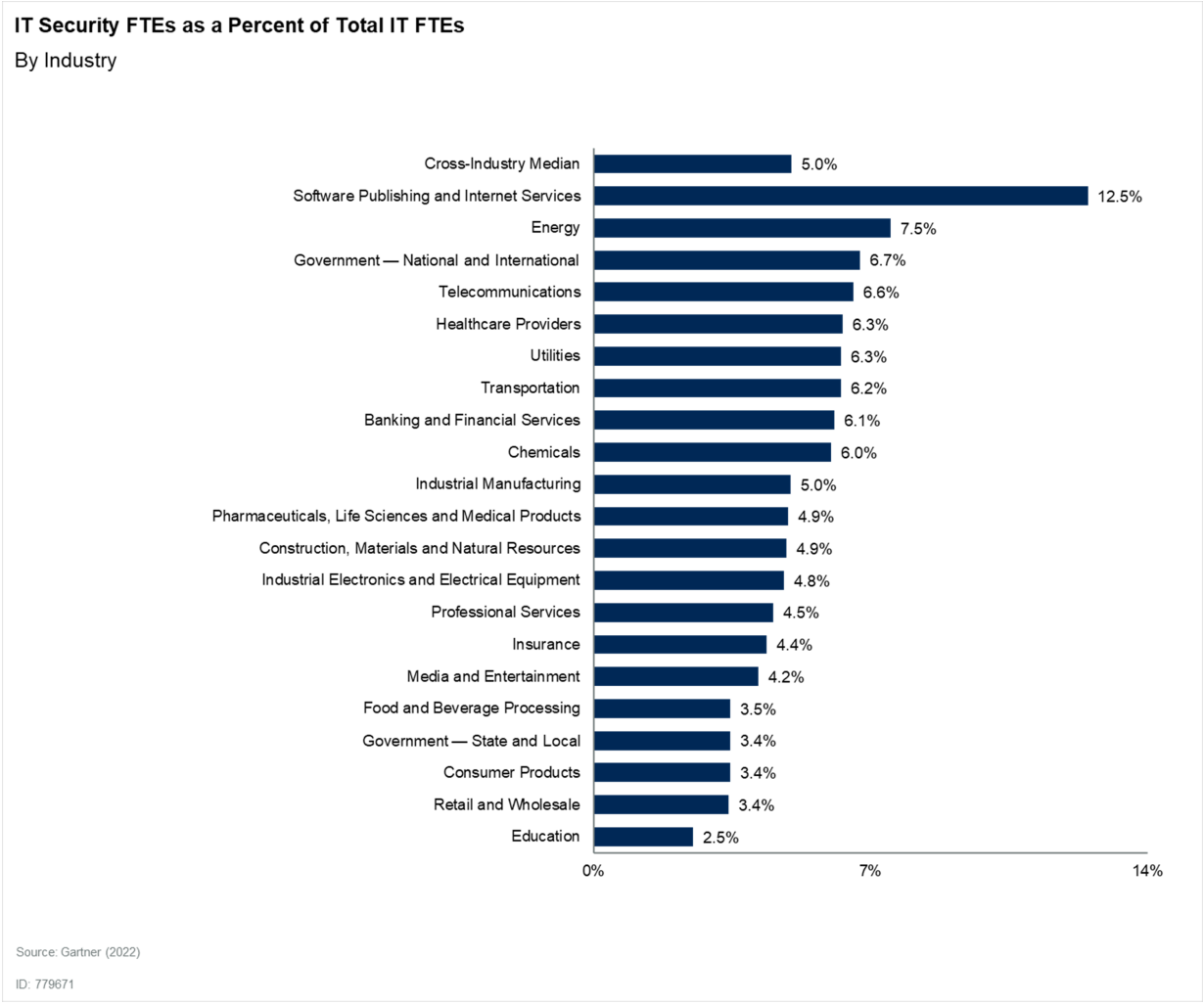


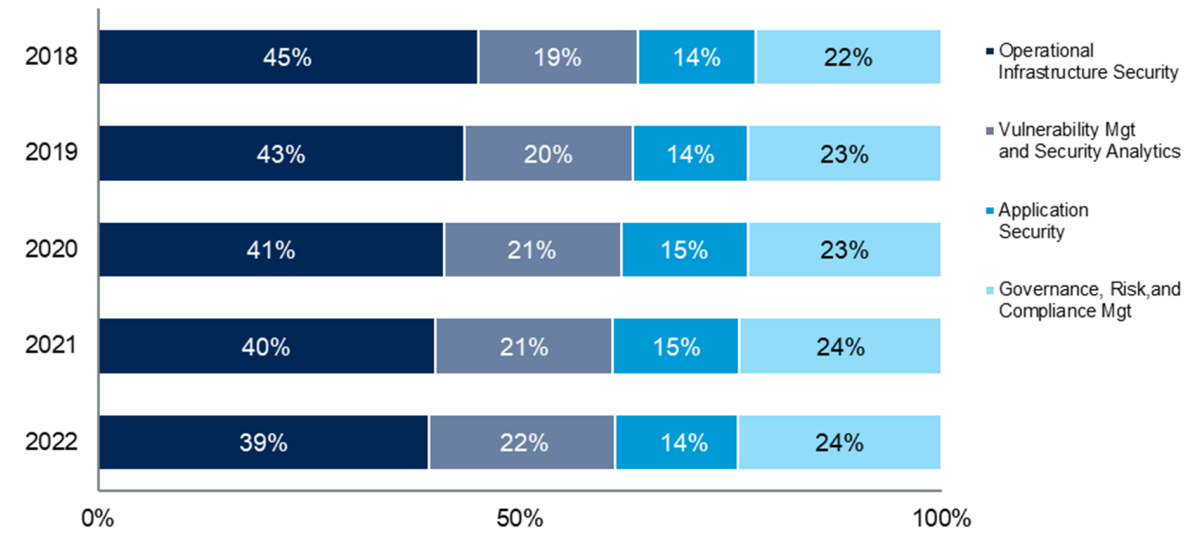
Figure 15: IT Security FTEs as a Percent of Total IT FTEs, by Industry



IT Security Staffing by Operation

IT Security staffing distribution by operation (Figure 16 & 17) is important as it indicates the personnel investments that go along with the IT Security spending distribution. Certain areas tend to be more personnel intensive such as governance, risk, and compliance management.

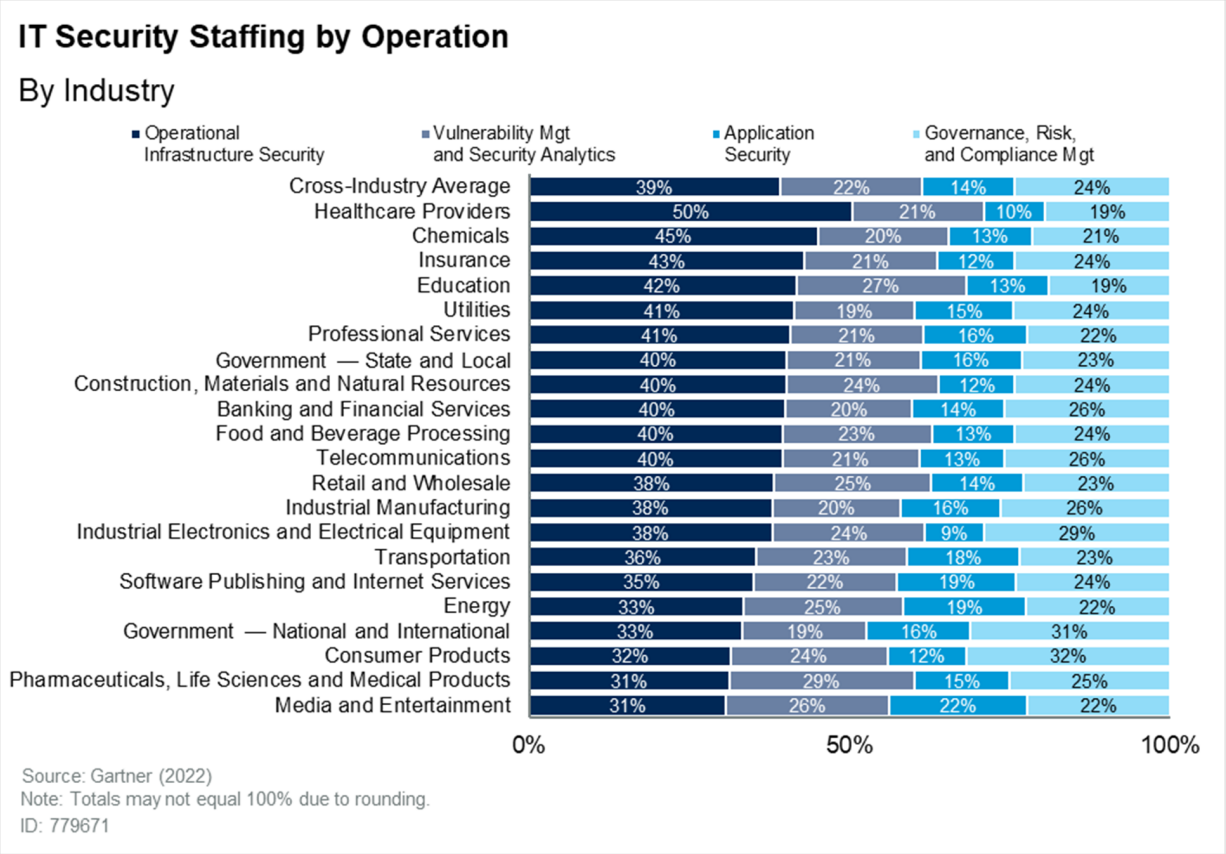
Figure 16: IT Security Staffing by Operation



Source: Gartner (2022)
Note: Totals may not equal 100% due to rounding.
ID: 779671

Gartner

Figure 17: IT Security Staffing by Operation, by Industry

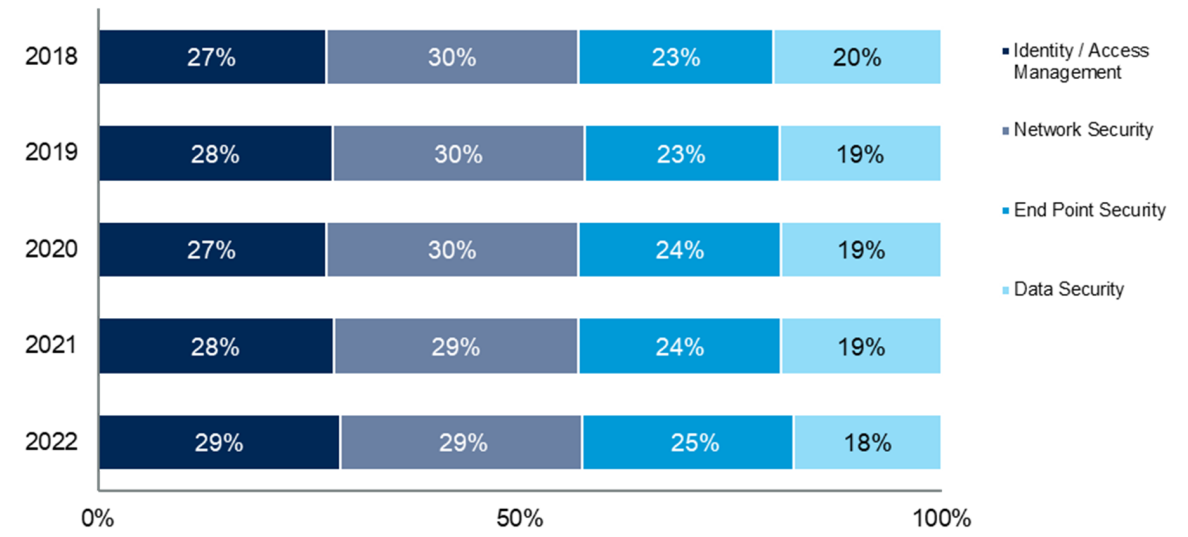


Gartner

Operational Infrastructure Security Staffing Distribution by Task

The distribution of operational infrastructure security staffing by task (Figure 18 & 19) provides an understanding of how security FTEs are dispersed to support the technology environments. This distribution helps to outline human resource allocations.

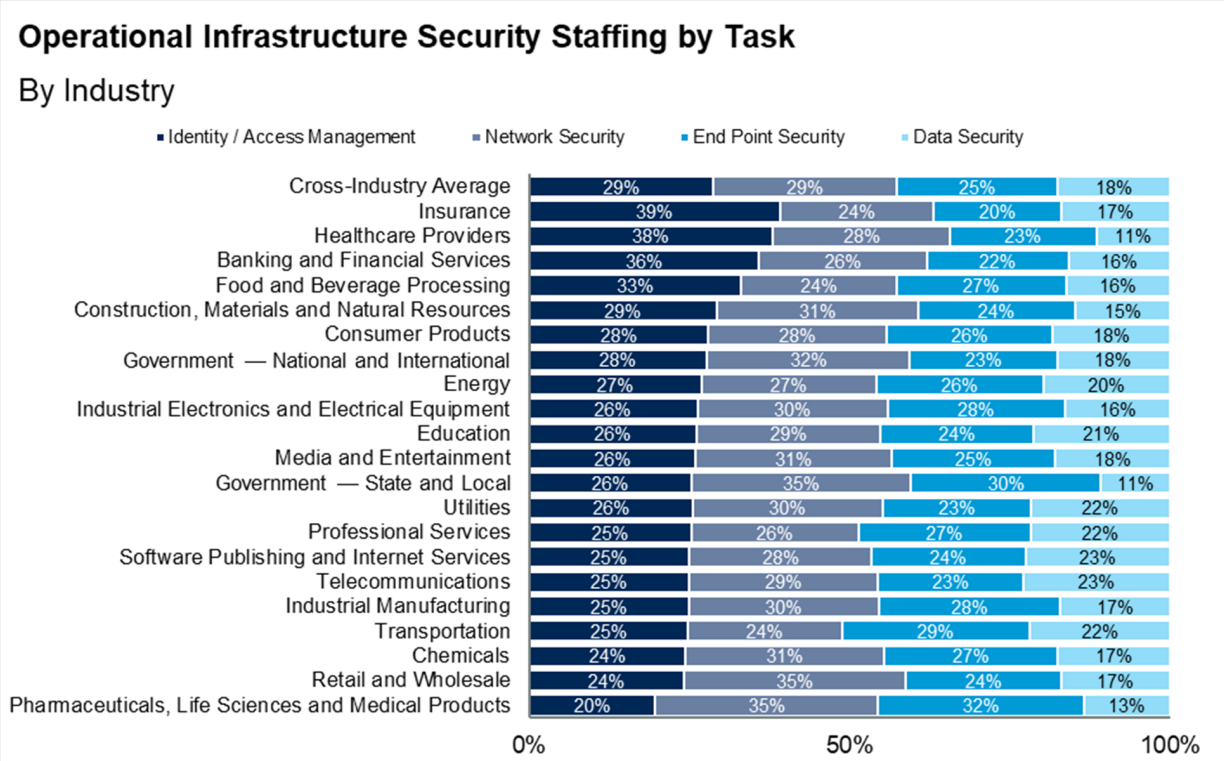
Figure 18: Distribution of Operational Infrastructure Security Staffing by Task



Source: Gartner (2022)
Note: Totals may not equal 100% due to rounding.
ID: 779671

Gartner

Figure 19: Distribution of Operational Infrastructure Security Staffing by Task, by Industry

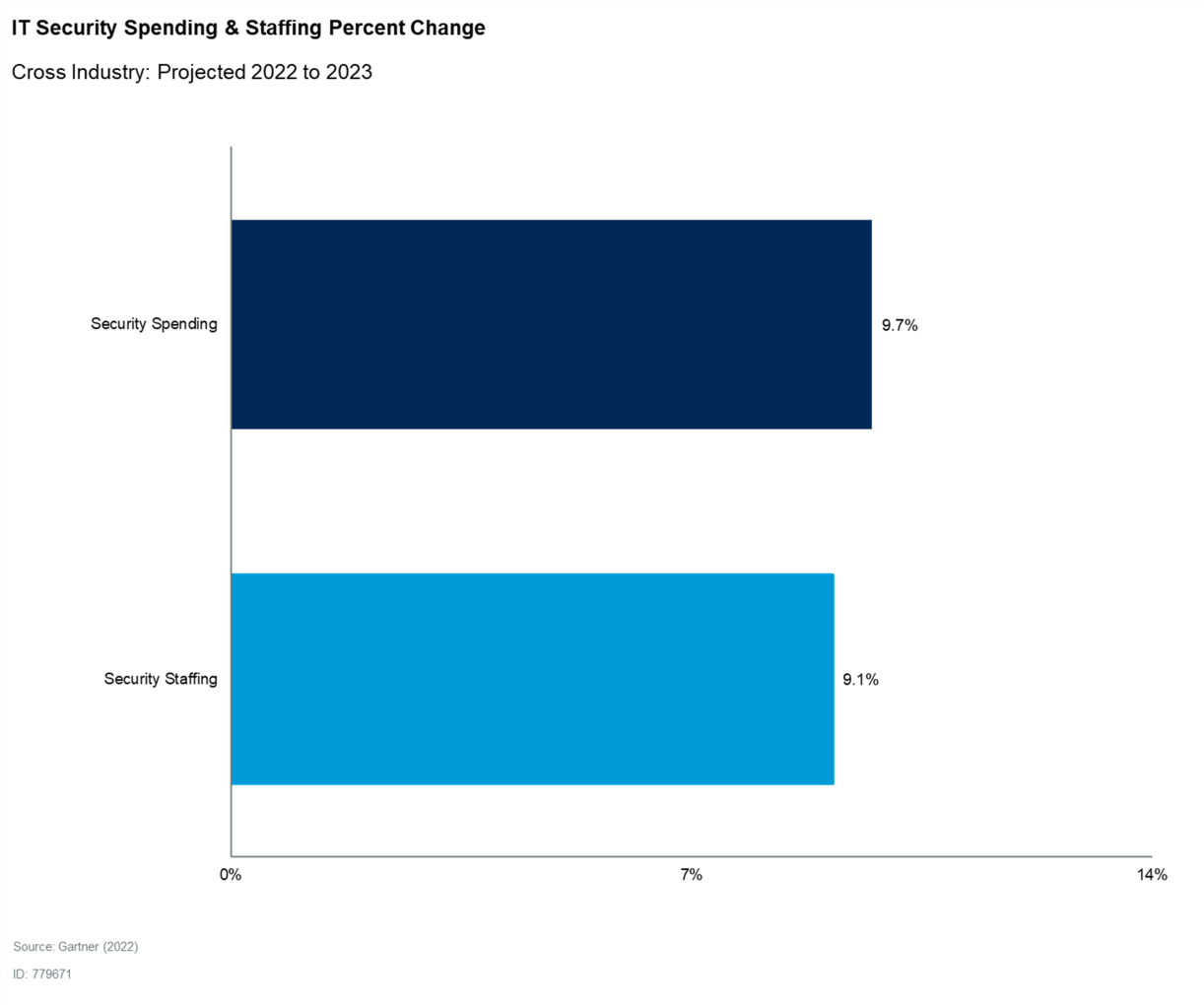


Gartner

IT Spending & Staffing: Projection

Figure 20 demonstrates projected growth in IT Spending & Staffing in 2023, compared to 2022. On average our respondents are expecting large growth in spending and staffing. It's important to remember that this data was collected during 2022 as economic conditions were shifting and that they will continue to shift throughout next year.

Figure 20: IT Spending & Staffing Projections



Conclusion

A successful IT performance measurement program communicates metrics that are important to a target audience. This remains true when communicating IT investments to the business. The metrics and benchmarks that Gartner has identified here provide a high-level view of current trends in IT by industry. They also reveal trends in business alignment, staffing, technology and outsourcing. They can be used to assist in communicating alignment with the business and in evaluating targets in key technology areas. They provide context for key business decisions and internal performance measures.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

IT Score for Security & Risk Management

Leadership Vision for 2022: Security and Risk Management Leader

Top Security in Cybersecurity 2022

IT Cost Optimization, Finance, Risk and Value Primer for 2022

Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer

How to Design a Security Champion Program

Security Program Management 101 — How to Select your Security Framework

About This Research

This research contains relevant database medians and ranges from a subset of metrics and prescriptive engagements available through Gartner Benchmark Analytics consulting-based capabilities.

Calculations were made using worldwide observations.

Evidence

IT Security Analysis Data Demographics by Environment Size: The niche subsector, business scale and tolerance to risk along with the future state strategy of each organization drive many of the variables required to understand the appropriate level of IT security investment required.

To offer some high-level insight into the data used for analysis, we have outlined the distribution of the data by revenue (Figure 21) and industry (Figure 22).

Sample: 947

Figure 21: Distribution of IT Security Data by Business Scale: Revenue Size

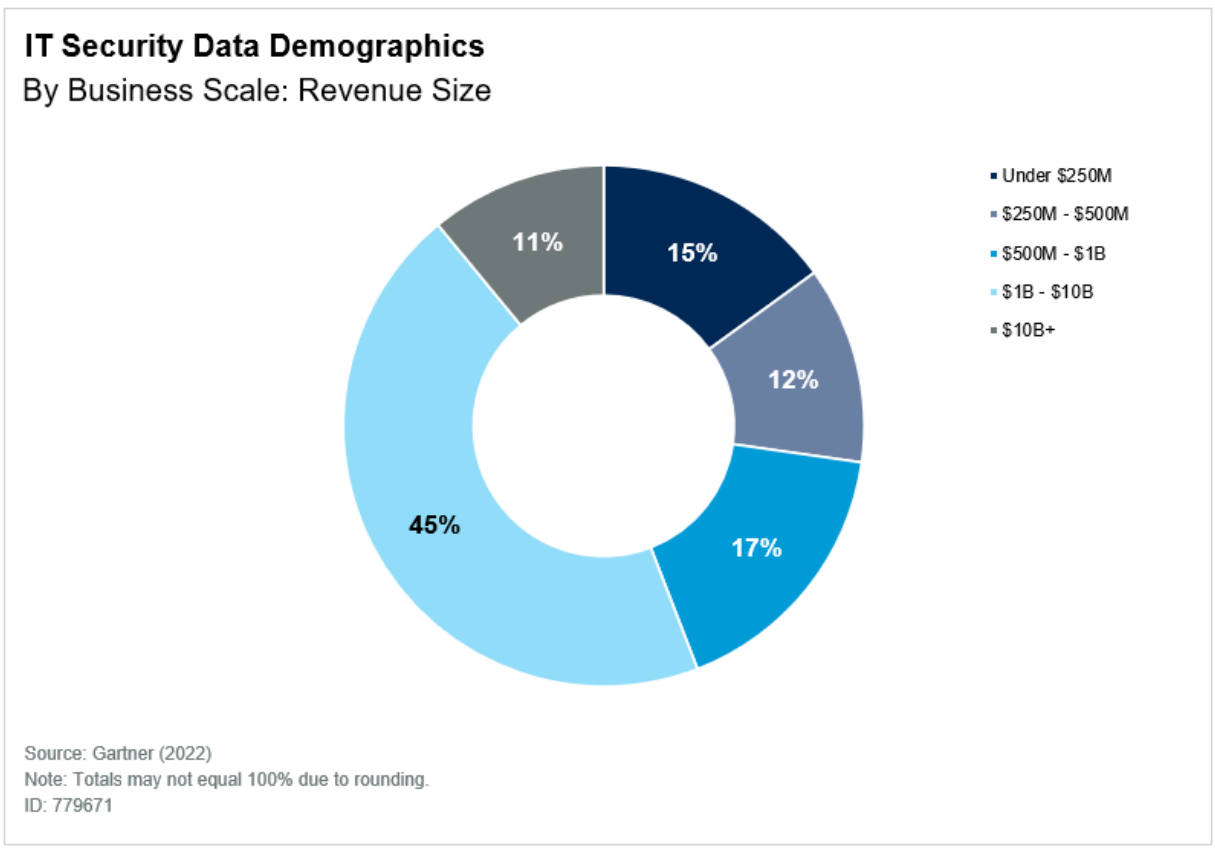
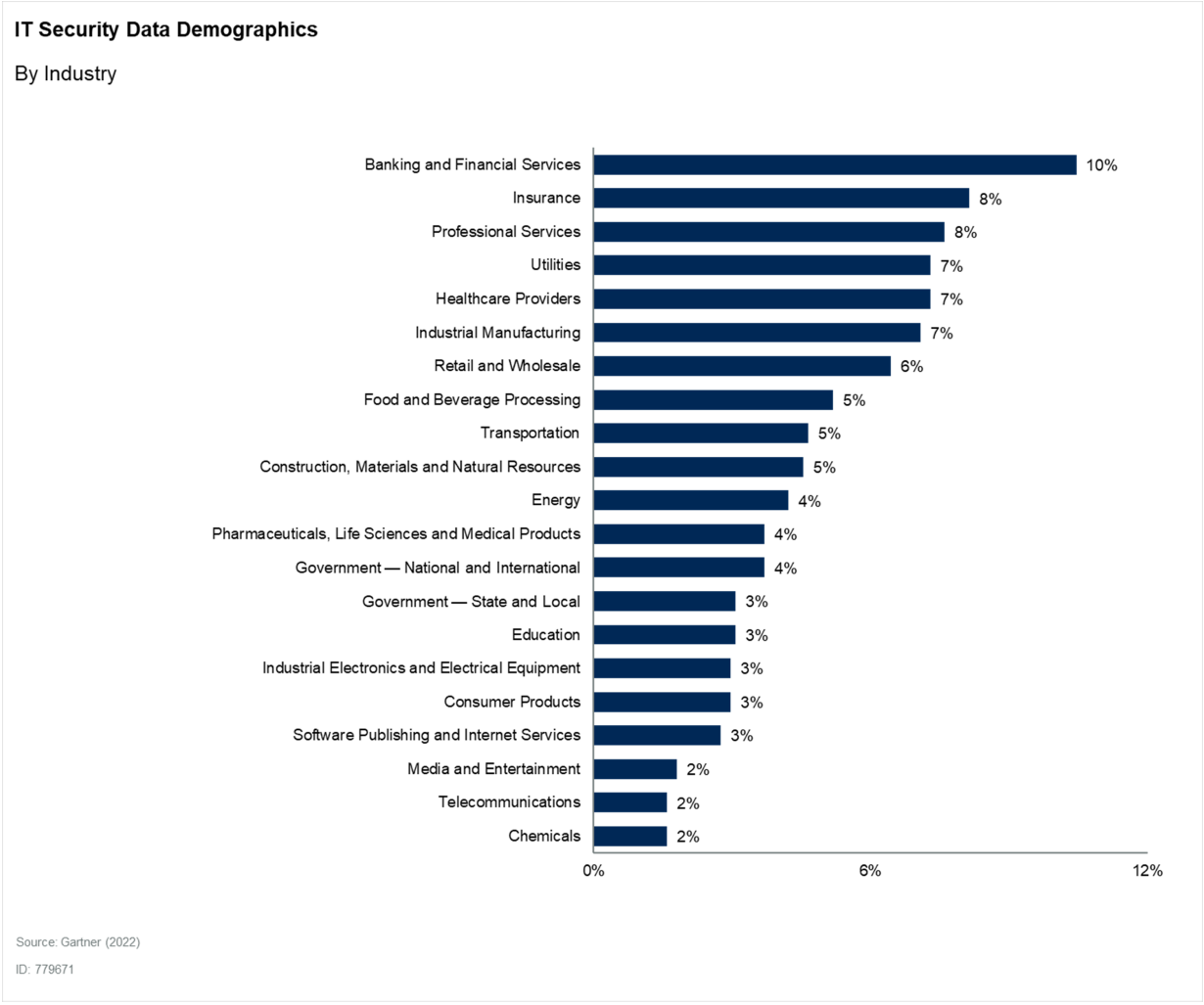


Figure 22: Distribution of IT Security Data, by Industry



Document Revision History

IT Key Metrics Data 2022: IT Security Measures — Analysis - 16 December 2021

IT Key Metrics Data 2021: IT Security Measures — Analysis - 18 December 2020