EMA
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Sponsored by:

baffle

CERBERUS SENTINEL

sumo logic

Using Compliance Budget to Advance Security Priorities

May 2022 EMA Research Report

Christopher M. Steffen, CISSP, CISA
Managing Research Director, Information Security, Risk and Compliance Management

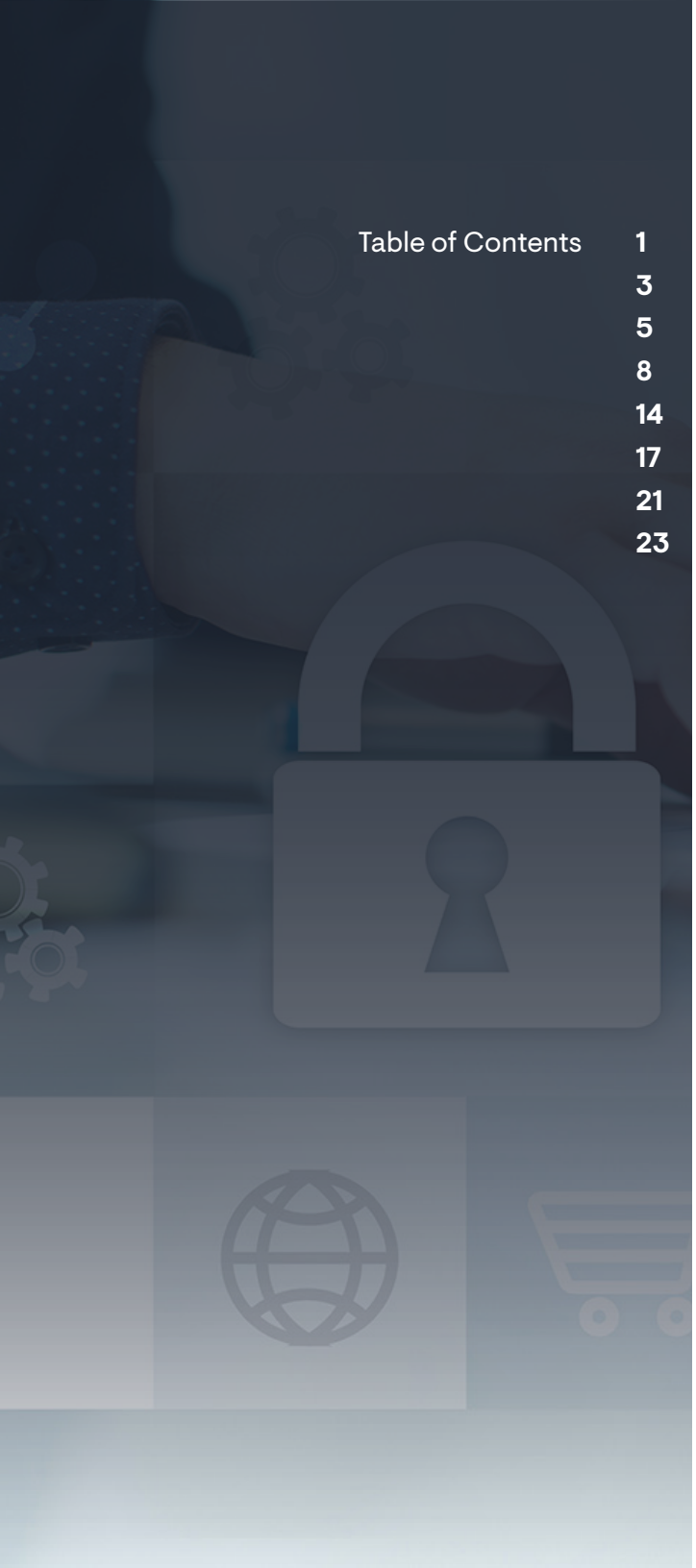


Table of Contents

Introduction

Organizations continue to prioritize security and security spending, but that spending is often at odds with a more pressing business priority: regulatory compliance. Regardless of the industry vertical, all businesses are required to deal with a certain amount of regulatory compliance or vendor due diligence. For technology leaders, the best solution is to partner with compliance/risk/governance teams to address compliance control gaps while advancing the company's security priorities. One of the best approaches to this solution is to implement security resolutions that directly address remediation items from a control gap list, or by finding dual-purpose security solutions that solve a compliance-related challenge while augmenting security capabilities.

This report examines how companies are prioritizing information security and compliance priorities, including which leaders control information security spending, how compliance-related priorities have shifted the overall security strategy of the organization, and the solutions and tools on which organizations are focusing their technology spending. It also specifically looks at how data security/privacy-related regulations have influenced the direction of security priorities as more companies and governments enact data privacy controls.

In this research study, Enterprise Management Associates polled 204 technology and business leaders in North America, representing organizations from more than ten different industry verticals. Nearly 83% indicated that an employee in their organization was responsible for information security (as opposed to an outside consultant or third party), and 88% stated that their IT audit and compliance function is conducted internally as well.

Key Findings

Trends

- **39%** said that multiple environments pose the greatest challenge to IT audit/compliance
- **38%** indicated that data security/privacy was the greatest security challenge in their organization
- **25%** stated that information security projects are dependent on compliance projects
- **89%** indicated that the priorities of the security and compliance teams were aligned
- **85%** stated that the security tools used adequately address compliance considerations
- **40%** of organizations have postponed security projects to address regulatory compliance concerns
- **76%** said that compliance has completely or significantly shifted their security strategy
- **68%** believe their regulatory compliance programs are a competitive differentiator

Data Security/Privacy

- **75%** believe that a data privacy program would be a competitive differentiator in their space
- **59%** indicated that data privacy regulations have impacted their approach to security
- **75%** stated that they are using existing tools or evaluating new tools to address data privacy

Security/Compliance Spending

- **47%** indicated that IT owns the security budget
- **11%** stated that compliance is the security budget owner
- **14%** said that compliance drives information security priorities

Voices of the Survey – Respondent Quotes

Select Open-Ended Responses:

Compliance and audit are main functions of our organization that are taken very seriously. We are actively increasing our budget annually by minimum 10%. We take a straightforward, results-driven approach and strive for excellence.

Everyone works together and shares the responsibility to make compliance their priority. Rather than receiving high-level guidance from an authority figure, the group shares the responsibility for achieving and demonstrating compliance. It's the we're in this together approach.

In our organization, we consider IT compliance and audit to be a top priority. We have hired a third party who carries on unbiased checks on the company's operations. Various intermediate checks are internally done too to keep the operations on track and secured.

We have an automated approach to IT compliance. We always try to make sure that we have the best plan in place to deal with cybersecurity and other regulatory issues.

We seek to comply with all industry regulations to ensure customer data is secure, and we adhere to insurance regulations. We partner with a third-party vendor to help us keep up to date with constantly changing insurance and data privacy regulations.

An extensive variety of automated reporting has been set up in addition to other things. This is used to evaluate the strength and thoroughness of the compliance process, security policies, user access controls, and risk management procedures during the course of the audit.

Information technology compliance is at the forefront of how our own organization regulates technology strategy. Technology spend for consultation and the products and services we choose to use must be compliant with consideration directed toward honoring our commitment.

We deal with a third-party audit company that sits down yearly with our IT/management team, and we review a set list of criteria. We look at our employee team changes (security and access requirements), as well as noting team members who have left the company and we have revoked their security clearances. We look at our control measures, security software changes, and internal and remote systems in place.

IT auditing occurs formally under an institutional auditor on an annual basis – this includes finance, performance, operations, and compliance. Meanwhile, we undertake a variety of regular (monthly/quarterly) processes of our systems to ensure that we are prepared for our institution's formal audit.

It is where we like to be on top of all the time. We feel that our approach to IT gives our company its leading edge over our competitors. Not to brag, but we feel from the research we have done that we lead in IT technology by 15% over our competitors.

Information Security and IT Audit/ Compliance Trends

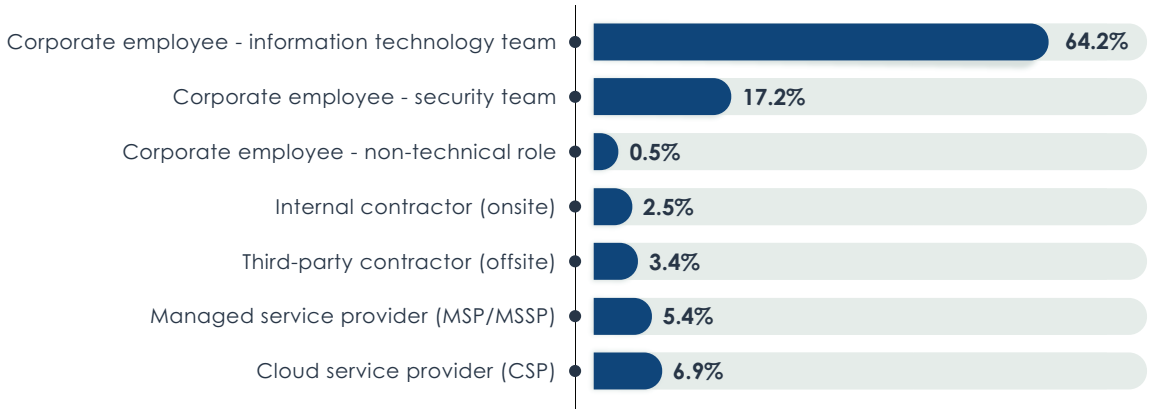
Analysis:

When looking at the spending drivers for an organization, it is often telling to know who is providing the functions. In this survey, almost 82% indicated that a corporate employee provides their security administration, and over 88% said that their IT audit and compliance was a corporate employee.

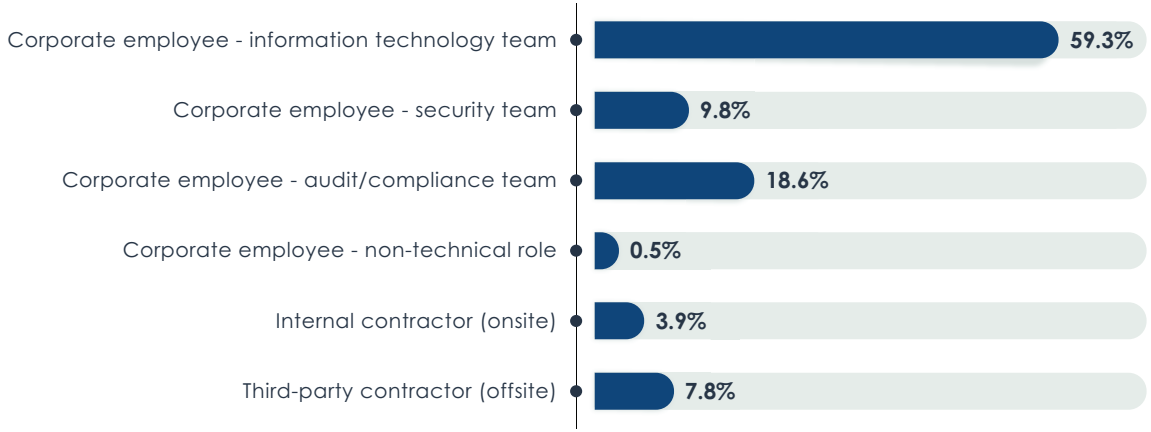
Commentary:

There is little doubt that in a perfect world, nearly all organizations would prefer to have their security and IT audit functions run in house. Talent shortages and resource constraints often require organizations of every size to outsource these functions to focus on other priorities. It was surprising that more organizations do not outsource their IT compliance activities, as most vendors and regulatory frameworks require a third-party validation of results. On the security side, it is still extremely concerning that almost 7% of organizations believe that their cloud provider is responsible for their organization's security, demonstrating a fundamental lack of understanding of the shared responsibility model for security between the cloud providers and the customers.

Who provides security administration for your organization?



Who provides IT audit/compliance functions for your organization?



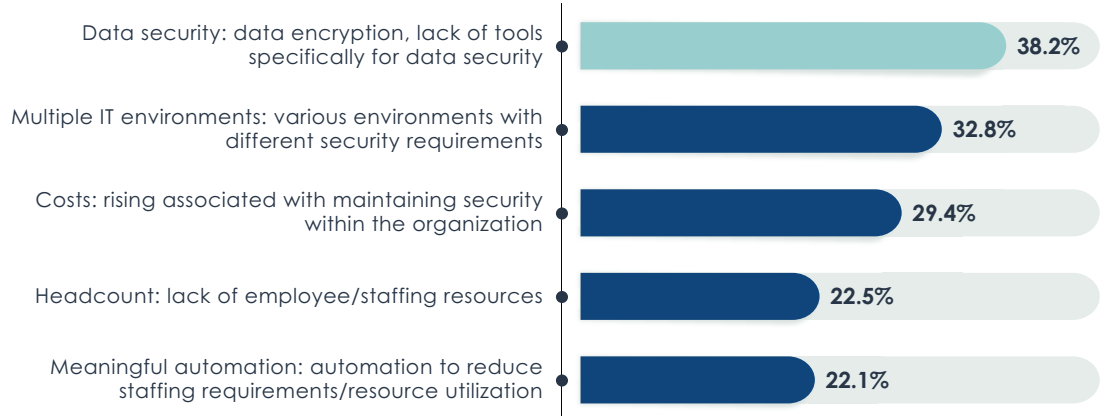
Analysis:

Every organization has challenges they would rate as the most significant one facing their organization. Data security – the tools and encryption of data – was rated as the greatest security challenge, while dealing with an organization's multiple IT environments and the controls that govern those environments is considered the greatest challenge in the IT audit/compliance space.

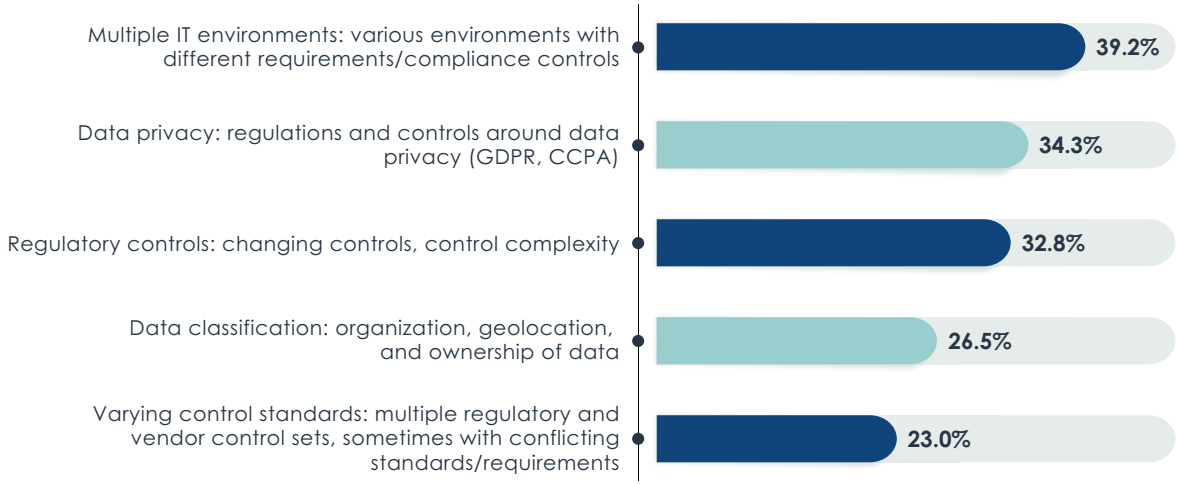
Commentary:

The regulations around data security/privacy are top of mind for most IT practitioners and technology leaders. How to best deal with the various control frameworks and how they are applicable to their organization is an extremely high priority for nearly every organization of every size and every vertical. Even starting a data security program is a challenge: understanding an organization's data estate – where it is located, who owns the data, how is it classified – is a daunting task, and many organizations are prioritizing addressing this challenge above all others.

What is your organization's greatest information security challenge?



What is your organization's greatest IT audit/compliance challenge?



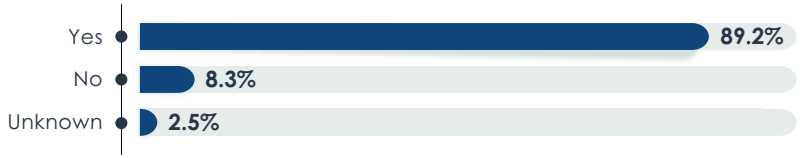
Analysis:

Who is calling the shots for information security? In some instances, those surveyed indicated that information security and IT compliance priorities were generally aligned (89%). In other instances, one-quarter of the information security projects were dependent on compliance involvement. Forty percent responded that security projects had been suspended to address compliance-related priorities.

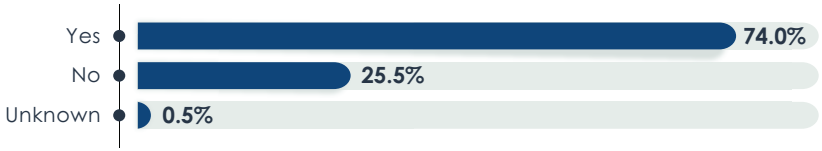
Commentary:

While it appears that most organizations have aligned their compliance and security teams, there is still a question about which organization has the highest priority in the minds of business leaders. There is little resistance about the need to have alignment between security and compliance, and how both must be aligned with business needs and requirements. When presenting a unified front, security and compliance working together can be transformational for technology maturity for the organization.

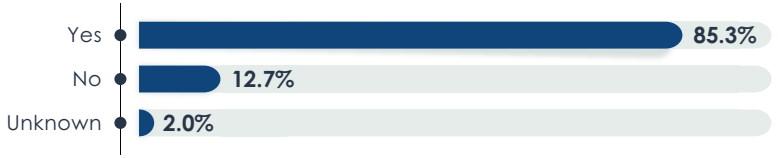
Are the priorities of the security team aligned with the priorities of the compliance team?



Are security projects independent of compliance projects?



Do the security tools your organization currently uses adequately address compliance/audit considerations?



Has your organization postponed IT and/or information security projects to address compliance-related concerns?

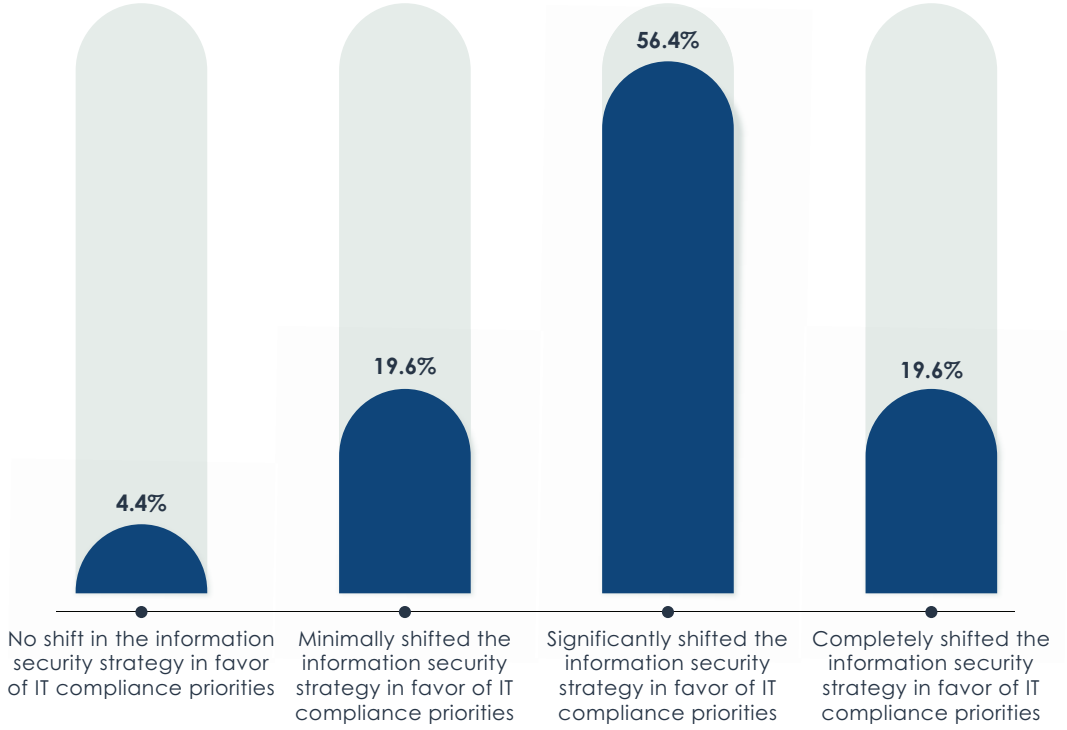
Analysis:

It comes at little surprise that compliance has impacted the information security strategy for the organizations surveyed. In this case, over 93% indicated that their strategy had shifted to address compliance priorities, with nearly 20% sharing that their organization's security strategy had been completely changed to address compliance needs.

Commentary:

If you consider that compliance goals are generally aligned to business priorities, then the idea that the information security strategy has shifted to address BUSINESS priorities (instead of compliance priorities) may make more sense. Information security leaders can no longer choose projects and goals without addressing very specific business needs. Even some organizations' undirected security evaluations and research now come with the qualification that it must directly tie into regulatory control gaps or vendor due diligence requirements. Future security planning should also try to take into account the constant change in regulatory controls, staying ahead of requirements before they become emergencies or regulatory findings.

Have IT compliance priorities impacted your organization's information security strategy?



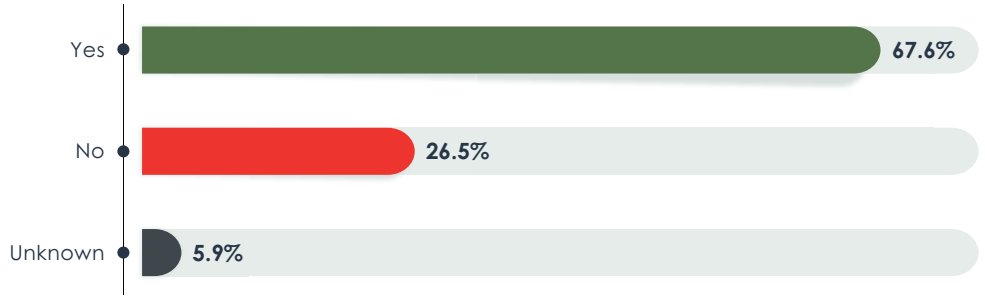
Analysis:

In many verticals, how the organization approaches compliance-related activities is viewed as a competitive advantage. From those surveyed, almost 68% looked at their compliance program as an advantage over their competitors, while three-quarters (75%) viewed their data privacy efforts as something that could be used as a competitive differentiator.

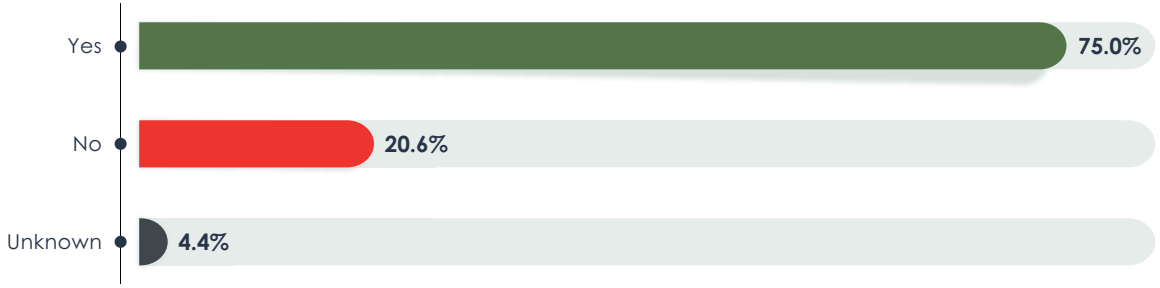
Commentary:

Most organizations view compliance and compliance-related activities as "the cost of business," something they have to do to conduct operations in certain markets. Increasingly, forward-thinking organizations are looking for ways to maximize their competitive advantage in their markets and having a best-in-class data privacy program or compliance program is something that more savvy customers are interested in, especially in organizations with a global reach. Compliance is no longer a "table stakes" proposition: comprehensive compliance programs focused on data security and privacy can be the difference in very tight markets and are often a deciding factor for organizations choosing one vendor over another.

Has your organization used or is your organization looking to use regulatory compliance programs as a competitive differentiator?



If your organization were to implement a significant data privacy program, do you believe that it could be a competitive differentiator in your space?



Data Security/Data Privacy

Analysis:

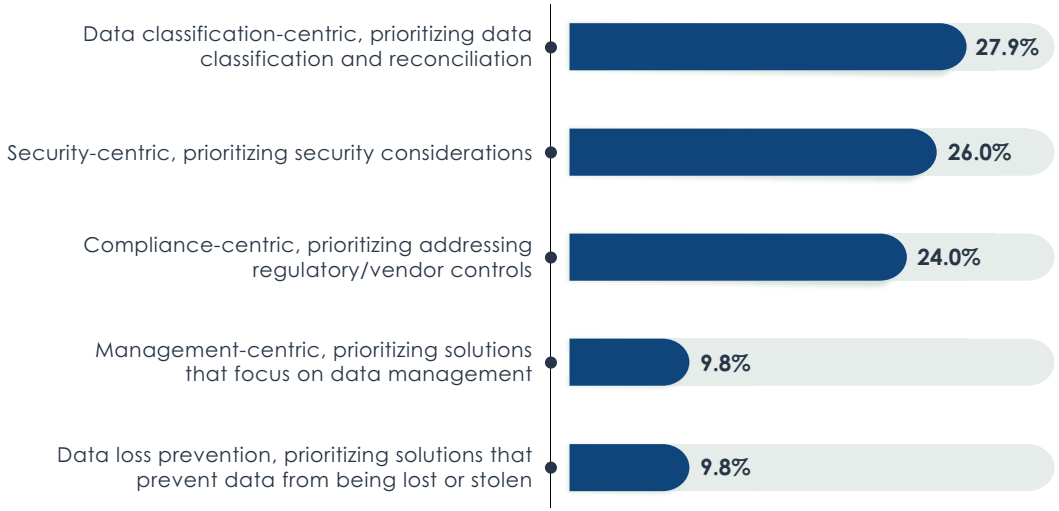
One of the hottest topics in information security and regulatory compliance is data security and privacy. Data privacy regulations, such as the EU's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA), are primary considerations for business and technology leaders. From those surveyed, almost 59% have altered their organization's approach to information security to address these data privacy regulations.

Commentary:

Protecting data – and all of the regulations and controls around data protection and privacy – are at the top of the concern list for nearly every security practitioner and technology leader, so it is little surprise that many organizations have altered their security strategy to address this priority. There are multiple approaches – each with valid rationale – to address these data privacy considerations. Ultimately, an organization's approach to data security and privacy will likely be determined by who has the greatest influence in the organization: information security and regulatory compliance likely have a direction, but operations and even executive management will also have a path or perspective. Vendors in the data security space would do well to consider all of the various personas that impact a data security/privacy decision.

Have data security/privacy regulations, such as GDPR or CCPA, impacted your company's security approach?

When considering the methods used by your organization to address data privacy, which of the following best describes the approach?



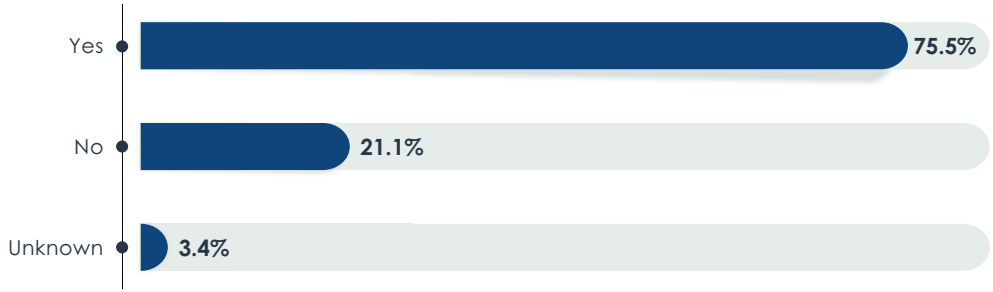
Analysis:

Since data privacy is a major consideration in nearly every organization, it stands to reason that the tools the organization purchases to address security controls must also have the ability to address data privacy considerations. Seventy-five percent of those surveyed indicated that they are looking at tools to address data privacy controls, and 93% said that it was very or moderately important that their security tools can be used for data privacy and other security controls.

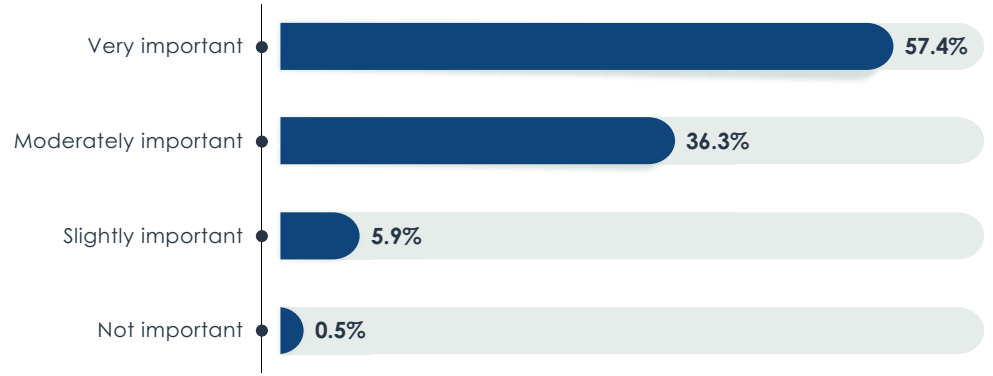
Commentary:

Data security/privacy concerns will be a primary motivator for security and compliance spending for the foreseeable future. As the impacts of privacy legislation become clearer (since there are additional rulings and findings based on the regulations), organizations will have a better sense of how and where to invest security and compliance resources to address these concerns.

Is your organization evaluating tools/using existing security tools to address data privacy considerations?



How important is it to your organization that the tools used to address data privacy are also used to address other security considerations?



Security/Compliance Spending

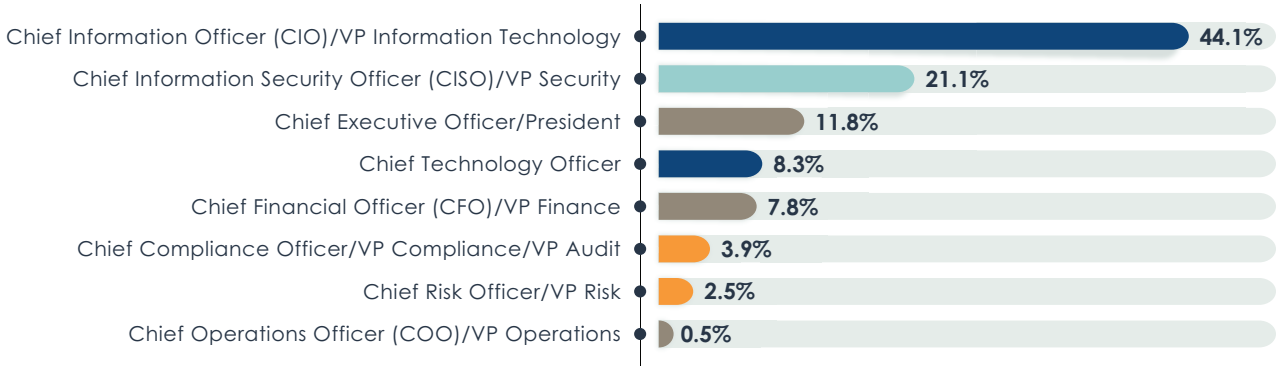
Analysis:

There are three "factions" or influencers when talking about technology, information security, and IT compliance-related budgets. For the organizations that participated in this survey, the Chief Information Officer was ultimately responsible for the budget for security and IT compliance investments. The CISO (for security) and the Chief Compliance Officer (for compliance) did have significant influence over their respective budgets, and there were plenty of other influencers that were part of the process.

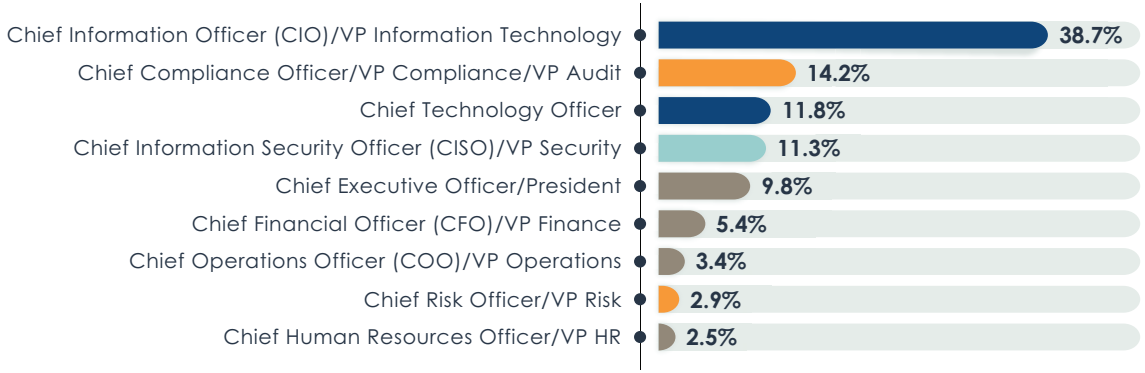
Commentary:

Technology budgets are fluid things. There are constant influences pulling for elusive technology resources, with information security and compliance only two of many groups that often fall under the larger technology budget. Those that influence where technology dollars are spent is not limited to just technology leaders: operations, finance, and business line executives all have priorities and projects to spend technology resources. Deciding where best to spend those resources is a constant juggle, with constantly changing variables and priorities all vying for limited dollars.

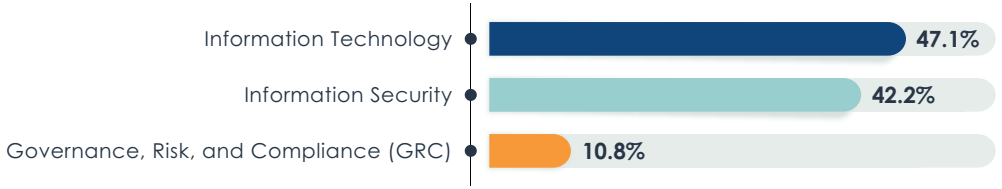
Who is the ultimate decision-maker for INFORMATION SECURITY investments?



Who is the ultimate decision-maker for IT AUDIT/COMPLIANCE investments?



Which department in your organization owns the security budget?



Analysis:

Organizations are spending on security and compliance-related priorities. In fact, 75% of those surveyed showed that there was an increase in spending in IT, information security, and IT compliance over previous years. Security showed the largest increases and the least amount of decrease over previous budgets.

Commentary:

IT spending continues to rise as organizations see the critical nature of technology to run their operations. Information security is also seeing significant increases, with only 1.5% indicating that they had decreased their security budget from previous years. Compliance still exerts significant influence on how those budget dollars are spent within most organizations.

How much does your organization budget annually for the following?

	$0	$1 - $5,000	$5,001 - $50,000	$50,001 - $500,000	$500,001 - $5,000,000	Greater than $5,000,000
Information Technology	0.5%	4.9%	26.5%	30.9%	27.9%	9.3%
Information Security	0.5%	5.9%	27.0%	32.8%	28.4%	5.4%
Information Technology Audit/ Compliance	1.0%	6.4%	29.4%	38.7%	20.1%	4.4%

How would you evaluate the FUTURE budget annually for the following?

	Significantly increasing (over 20% increase)	Moderately increasing (10-20% increase)	Slightly increasing (0-10% increase)	No change over previous years	Slightly/ Moderately decreasing (0-20% decrease)
Information Technology/IT Consulting	7.4%	33.8%	42.2%	14.2%	2.5%
Information Security/ Security Consulting	13.2%	30.9%	43.6%	10.8%	1.5%
IT Audit and Compliance/ Third-Party IT Auditors	7.4%	24.0%	42.2%	23.5%	2.9%

Analysis:

As shown in the tables, spending on data security/privacy tools represents a significant investment for those surveyed, and point solutions (tools that only solve one particular problem) are seeing the least amount of significant investment. On the solutions side, data privacy solutions are of most interest to those surveyed, and red team/blue team services are the least.

Commentary:

There's a lot of data on these tables, and there's something that can point to nearly every type of security and compliance solution and tool in the market. Not surprisingly, data security/privacy solutions are highly rated and single point solutions are not. Nearly every category had significant investment and nearly every category had increases in investment, showing how strong and important the security and compliance programs are to business leaders.

Please rate how your organization currently spends/plans to spend on the following.

Tools	Current Spending				Future Spending			
	Significant Investment	Minimal Investment	Minor Investment	No Investment	Significant Investment	Minimal Investment	Minor Investment	No Investment
Single solution/point solution security tool	41.7%	40.2%	15.2%	2.9%	38.7%	48.0%	10.8%	2.5%
Security management suite/multi-solution tool	44.1%	43.1%	12.7%	0.0%	52.5%	35.3%	10.8%	1.5%
Compliance management	45.6%	39.7%	13.2%	1.5%	40.2%	41.7%	2.5%	15.7%
Vulnerability scanning solution	38.2%	39.2%	19.1%	3.4%	44.6%	41.2%	13.2%	1.0%
Data security/data privacy management	50.5%	33.3%	14.2%	2.0%	46.1%	39.7%	13.7%	0.5%
Vendor management solutions	31.4%	41.2%	19.6%	7.8%	40.7%	38.2%	18.6%	2.5%
Risk management solutions	35.3%	48.5%	15.7%	0.5%	40.7%	42.2%	15.7%	1.5%
Data protection solutions (BYOK, tokenization, masking, encryption)	43.6%	41.2%	14.2%	1.0%	43.1%	43.1%	11.8%	2.0%

Solutions	Current Spending				Future Spending			
	Significant Investment	Minimal Investment	Minor Investment	No Investment	Significant Investment	Minimal Investment	Minor Investment	No Investment
Compliance management	38.2%	46.1%	14.7%	1.0%	48.0%	38.2%	12.3%	1.5%
Cyber-threat hunting services	44.1%	35.3%	17.2%	3.4%	44.6%	40.2%	14.2%	1.0%
Data privacy/data loss prevention	50.0%	31.4%	17.6%	1.0%	48.0%	35.8%	15.7%	0.5%
Incident response	40.2%	40.7%	17.2%	2.0%	39.2%	42.6%	16.2%	2.0%
IT audit/certification	35.8%	46.6%	17.2%	0.5%	38.7%	45.6%	14.7%	1.0%
Managed security solutions provider (MSSP)	36.8%	39.2%	20.1%	3.9%	31.9%	47.5%	17.6%	2.9%
Penetration testing/social engineering	33.3%	43.1%	20.6%	2.9%	35.8%	46.6%	14.2%	3.4%
Red team/blue team	23.0%	42.6%	21.1%	13.2%	29.9%	37.3%	22.1%	10.8%
Risk management services	34.8%	43.1%	19.6%	2.5%	34.3%	48.5%	15.2%	2.0%
Third-party risk management	31.4%	44.1%	18.6%	5.9%	42.2%	41.7%	12.7%	3.4%
Vendor management	31.4%	42.6%	21.1%	4.9%	35.3%	44.1%	17.6%	2.9%

EMA Perspective

In recent years, information security has taken a much more active role in shaping organizational priorities. You only need to turn on the evening newscast to see the latest security breach or ransomware attack. These events are not lost on the board room and business leadership, and technology leaders are forced to provide answers about how their organization is not vulnerable to those kinds of attacks: "we are protected."

Enter the IT compliance team. Armed with regulatory frameworks and controls, it holds the organization accountable for the "we are protected" claims with demonstratable proof of protection and adherence to security and technology best practices. It is of little wonder why there has always been a certain amount of friction between the information security team and the compliance team in an organization, as one is often charged with holding the other's feet to the fire, and no one likes that.

Still, it doesn't have to be that way. This survey shows that the attitudes of these teams is starting to shift and synchronize for the betterment of the company. As organizations continue to spend budget and resources on information security and compliance, aligned priorities on how best to spend those dollars is critical, and appears to be happening.

Throughout this survey, there are three themes that continue to repeat.

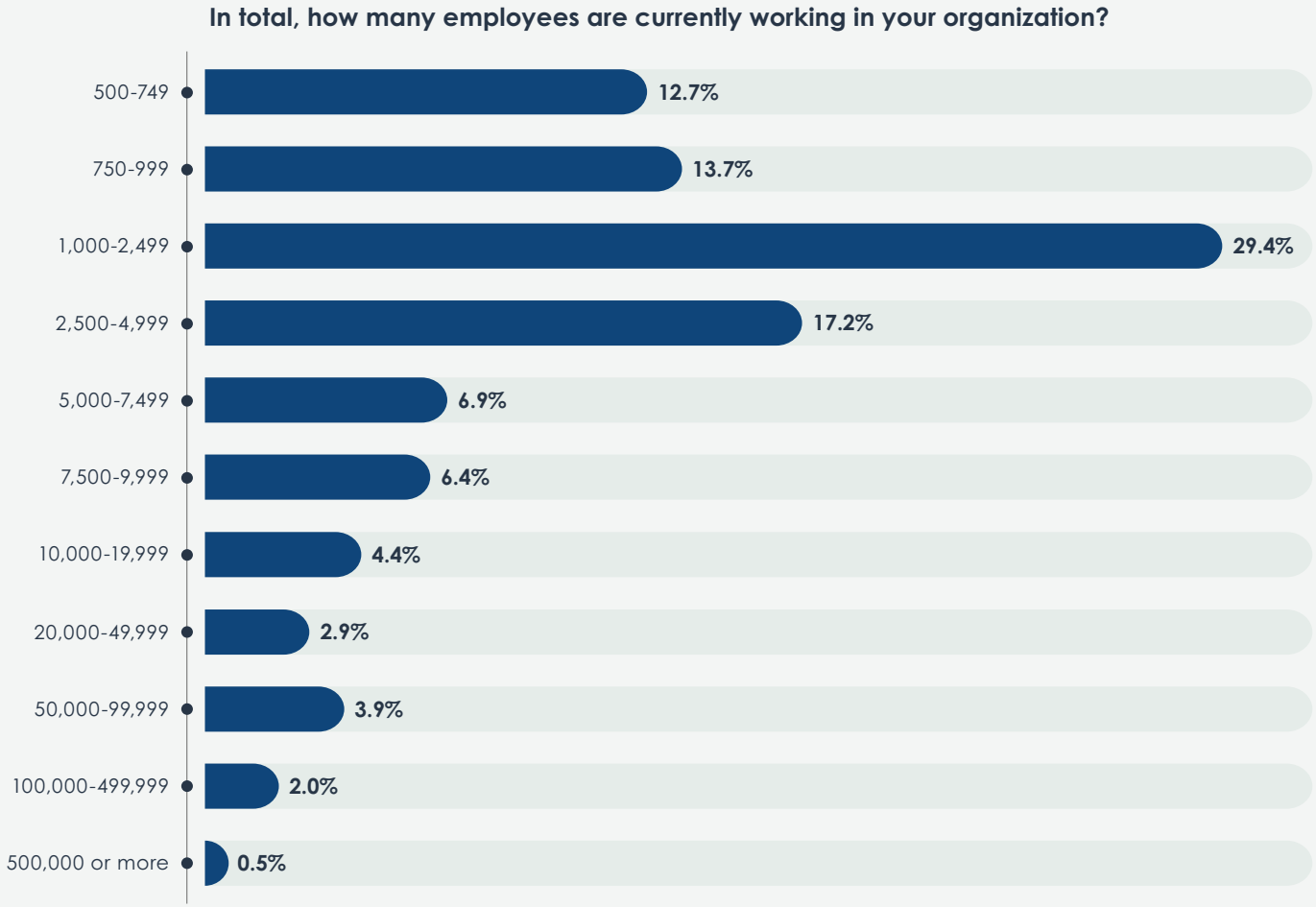
- **Technology spending is increasing, but it is complicated:** In the technology division of most organizations, there are plenty of influencers trying to spend limited technology dollars. Even funds specifically earmarked for security or compliance-related projects often have various approvers or collaborators that need to be appeased. Gone are the days of discretionary security or compliance spending, and while technology, security, and compliance budgets are all increasing, it always comes with strings attached. The best situation is when security and compliance priorities mesh to create a unified strategy for spending – one that addresses regulatory control gaps while increasing the organization's overall security posture. Security solution vendors would do well to market their tools with this in mind.
- **Alignment of security and compliance is a good thing – for everyone.** Simply put, security and compliance are better together than competing. When security and compliance have a unified strategy and vision, every department and employee within the organization benefits, as does the business customer. It also allows security to focus on real threats – the bad guys trying to steal data and cause harm to the organization – instead of the perceived threats – the compliance team are the bad guys, and they are trying to take over the world. There are not enough resources for this kind of infighting and diversion.
- **Overcoming attitudinal barriers to address ever-changing threats and regulations.** Changing the culture from "team vs. team" to "us vs. the REAL bad guys" is difficult, but necessary. Never does an organization want to be LESS secure, but organizational security can only be achieved by overcoming attitudinal differences and concentrating on the constantly changing threat landscape, increasing regulatory scrutiny (for companies of EVERY size and shape) and external pressures (like the lack of security talent, global instability, and new work culture challenges). When information security and IT compliance are working together to combat these challenges, there is a chance they might win. If they are fighting among themselves, they don't stand a chance.

Being able to quantify some of the ideas and statistics that were already known is a great thing for most and allows partitioners and leaders to present their projects and strategies with confidence knowing that directionally, they make the most sense. This researcher has always known how important it is for security and compliance teams to work together as a unified force, and the research proves that to be the case. Vendors that demonstrate how their solutions contribute to improving this synergy will be the ones awarded with the sale. Organizations that embrace information and compliance harmony will be leaders in their space, able to grow their businesses without the internal strife that usually accompanies these divisions and propel the company forward.

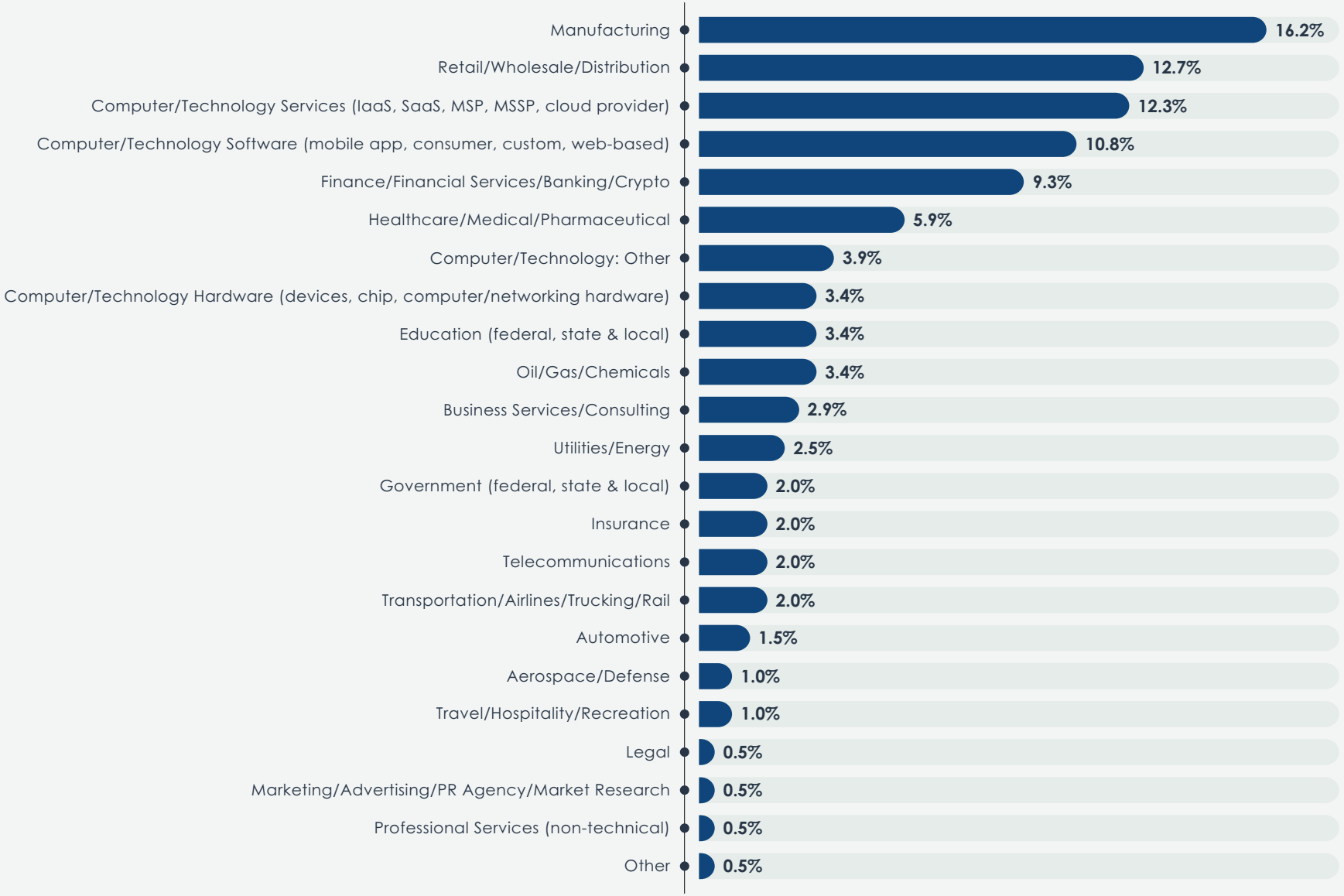
Research Methodologies and Demographics

Which of the following BEST describes your specific role?

Title	Raw Number	Percentage
IT Director/IT Manager/Supervisor (or equivalent)	63	30.88%
CIO/CTO/VP Information Technology	48	23.53%
Corporate/Line of Business Vice President (VP/AVP/SVP/EVP)	18	8.82%
Corporate/Line of Business Exec. Leadership (CFO, COO, CAO, Practice Lead)	10	4.90%
Information Security Director/IS Manager/Supervisor (or equivalent)	8	3.92%
IT Project/Program Manager	8	3.92%
CISO/CSO/VP Information Security	6	2.94%
IT Director/Manager (other)	6	2.94%
Chief Data Officer	5	2.45%
Director of Development/Engineering/Programming	5	2.45%
IT Service Manager/ITSM Team Leader	5	2.45%
Corporate/Line of Business CEO/President/Board of Directors	4	1.96%
VP Development/Engineering	3	1.47%
Director of IT Audit/Compliance	3	1.47%
Corporate/Line of Business General Counsel/Legal	3	1.47%
Director of Cloud Computing/Cloud Resources	2	0.98%
IT Administrator/System Administrator	2	0.98%
IT Architect	2	0.98%
IT Consultant/Integrator	1	0.49%
IT Business Analyst	1	0.49%
Help Desk/IT Support	1	0.49%
Survey Total Respondents	204	100%


In total, how many employees are currently working in your organization?
500-749
12.7%
750-999
13.7%
1,000-2,499
29.4%
2,500-4,999
17.2%
5,000-7,499
6.9%
7,500-9,999
6.4%
10,000-19,999
4.4%
20,000-49,999
2.9%
50,000-99,999
3.9%
100,000-499,999
2.0%
500,000 or more
0.5%

Which of the following best describes your organization's primary industry?



How many employees does your organization have in each of the following categories?

	0	1	2	3	4	5	6-25	26-50	More than 50
Information Technology	0.0%	0.0%	1.5%	0.0%	1.5%	1.0%	40.2%	32.4%	23.5%
Information Security	0.0%	0.0%	2.5%	4.4%	4.9%	2.9%	48.0%	27.0%	10.3%
Information Technology Audit/ Compliance	0.5%	1.5%	4.9%	2.9%	4.4%	9.8%	49.5%	18.6%	7.8%
Company-Wide Governance, Risk, and Compliance (GRC)	0.0%	1.0%	3.9%	4.4%	4.9%	9.8%	40.7%	23.0%	12.3%

About the Sponsors

SumoLogic

sumo logic

https://www.sumologic.com/

Nearly every enterprise undergoing digital transformation is building cloud-native applications to deliver new, digital experiences. The Sumo Logic Continuous Intelligence Platform™ provides real-time analytics and insights to help practitioners and developers ensure application reliability, secure and protect against modern threats, and gain insights into their cloud infrastructures. By delivering a SaaS analytics platform for cloud-native application observability and security solutions, Sumo Logic is empowering the people who power modern, digital business so they, in turn, can deliver reliable and secure digital experiences.

Cerberus Sentinel

CERBERUS SENTINEL

https://www.cerberussentinel.com/

Cerberus Sentinel is focused on cybersecurity, compliance, and the culture that drives success, acquiring world-class engineering talent who utilize the latest technology to create innovative solutions to protect even the most demanding businesses and governments against continuing and emerging threats. Our exclusive MCCP+ value proposition leverages the deep domain expertise of talent across our organization to create a culture of security that uniquely addresses the needs of each customer. We are a team of industry leaders who collaborate to solve complex cybersecurity challenges and meet strict compliance requirements, delivering a holistic approach that's product agnostic at scale.

Baffle

baffle

https://baffle.io/

Baffle protects data in the cloud via a "no code" and "low code" data security mesh. The solution provides universal data protection to secure data wherever it lives and as it is consumed in distributed data environments. Companies can control who can see what data with this security layer with no performance impact on the user experience. Proven in large-scale environments, only the Baffle Data Protection Service de-identifies sensitive information on the fly as it is processed in the cloud. With no application changes, security teams can move in lockstep with business initiatives to move more data and workload to the cloud faster. Investors include Celesta Venture Capital, National Grid Partners, Lytical Ventures, Nepenthe Capital, True Ventures, Greenspring Associates, Clearvision Ventures, Engineering Capital, Triphammer Venture, ServiceNow Ventures [NYSE: NOW], Thomvest Ventures, and Industry Ventures.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

1995 North 57th Court, Suite 120, Boulder, CO 80301 +1 303.543.9500 **www.enterprisemanagement.com**

4188.062122