

The State of Cybersecurity in the Association Industry

EXPERTS

Rick Bawcum
CAE, CISSP

Rene Shonerd
CAE, MEd

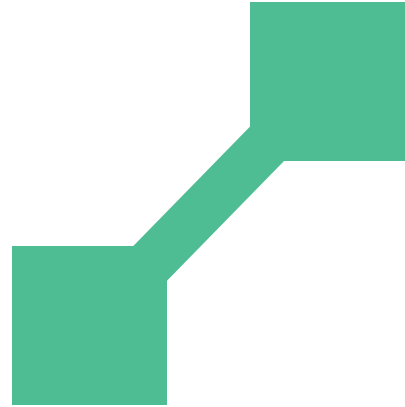


Table of Contents

- 3** Introduction
- 4** Executive Summary
- 5** Survey Results
- 9** Key Takeaways
- 10** Survey Results - Graphed
- 11** Best Practices
- 12** Policy Definitions
- 15** Survey Details
- 17** About Cimatri



Introduction

For over a decade, regulatory requirements have improved cybersecurity, but the basic guidelines established through these standards are just that: base level. And in the midst of the coronavirus pandemic and the resulting increase in remote work, many of those baseline standards are outdated.

Undoubtedly, there is now a gap between what is mandated from a regulatory perspective and what skilled risk managers consider adequate cyber-resiliency and risk management

Regulatory guidelines ensure that some level of privacy is maintained, but many organizations still see cybersecurity as an unnecessary added cost, despite its use in protecting confidentiality, integrity, and availability.

As such, they often forego investment into cybersecurity mitigations. (Read: These organizations have little to no buffer set in place to instill a level of digital resiliency.)

But that's why we're here.

We strip down the tech jargon, so you can fully assess the big-picture and craft research informed, actionable cybersecurity strategies.

To help you get started, we've surveyed a cross section of trade and professional associations so you can gain full insight into the state of IT security around the globe.



Executive Summary

In a digitally connected world, businesses are constantly exposed to new risks. In 2017, Aon's Global Risk Management Survey found that companies in North America view cybercrime and hacking as their number one risk.

Yet, even in a highly regulated industry, staying on top of compliance requirements alone does not equal security. Cyber-risk is dynamic and enterprise-wide, and security is an ongoing process that institutions must maintain with effective due diligence.

Moreover, in an effort to be all-encompassing, regulations can often be nonspecific, lacking the definition necessary for organizations to accurately implement security requirements. They also mandate a need for expensive changes that may, in turn, cause temporary disruptions or slowdowns in everyday business operations.

The bottom line? Regulations are rarely rigorous enough to create effective security solely on their own. Which presents yet another challenge.

Companies must meet baseline requirements but also tailor those requirements to suit the needs of their risk management profile. This, as one can imagine, is a painstaking task, requiring a scan of the current regulatory environment to be conducted alongside a practical cost / benefit analysis, which means organizations must balance compliance, risk management, and return on investment priorities.

Enter Cimatri's Survey on Association IT Security.

We surveyed associations of all geographic scopes, revenues, and staff sizes to determine how they are investing in cybersecurity.

Keeping in mind that few association executives can clearly define the steps needed to maintain compliance and mitigate risks, we designed the survey to specifically ask about the components needed to achieve compliance.

A recent study indicates that 92% of security breaches are human error, but many associations have taken a positive step towards their overall governance framework by initiating a cybersecurity training tool for staff.

But there is still more work to be done.

Use this survey as a guide to understand how your organization measures up, as well as view where you should expand your focus on cybersecurity.



Rich Bowe



The Results Are In

Phishing Tests

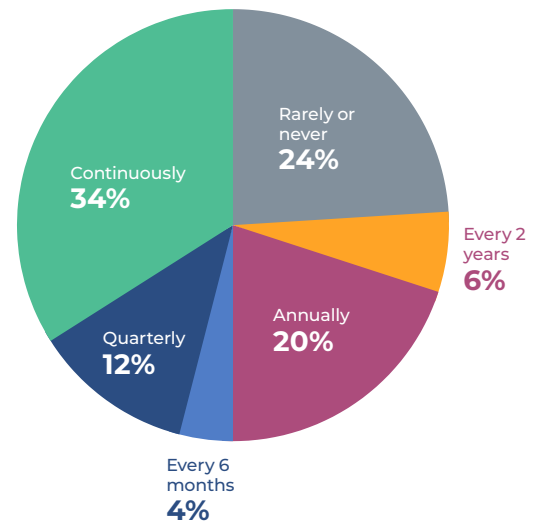
KnowBe4's recent benchmarking report shows that Not-For-Profits (including associations) have a phishing prone score of 39.2% within small organizations without security awareness training.

This indicates a high level of risk no hardware or software can mitigate. Rather, the vulnerability lies with your employees.

The most effective way to decrease that risk?

Train employees to identify phishing and social engineering attacks.

Do you conduct phishing tests for all employees?



Security Awareness Training

Most associations report engaging in some sort of security awareness training for employees, with 70% doing so at least annually.

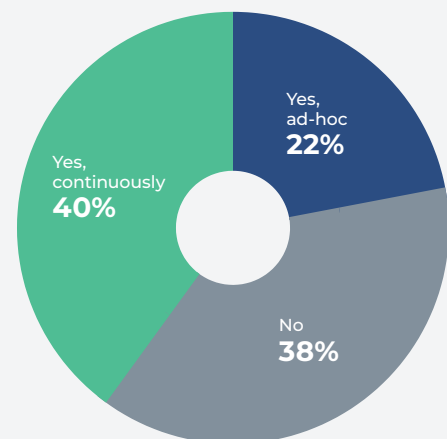
In the past few years, many associations subscribed to services that provide both phishing testing and online security awareness training. These programs are cost effective and make it simple to deliver quality training on an ongoing basis.

How can security awareness training help?

These trainings inform employees of:

- ✓ company policies and procedures
- ✓ sensitive data used in their role
- ✓ proper ways to store and transmit sensitive data

How often is security awareness training provided to existing staff?



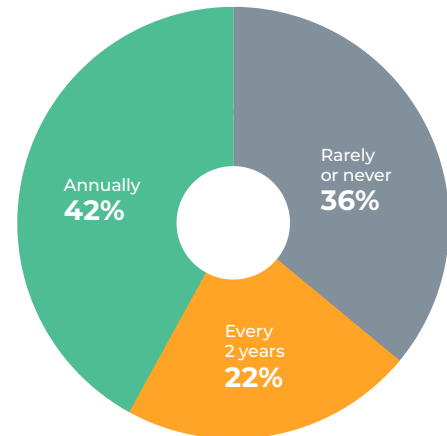
IT Risk Assessment

Risk assessments identify, estimate, and prioritize risk. The primary outcome from these conversations is a solid idea of what is considered an acceptable risk and what is not.

The challenge is to find an acceptable balance between the confidentiality, integrity, and availability of information assets.

64% of our survey respondents reported that their associations complete risk assessments annually or every two years.

How often do you conduct an IT risk assessment?



Cybersecurity Insurance

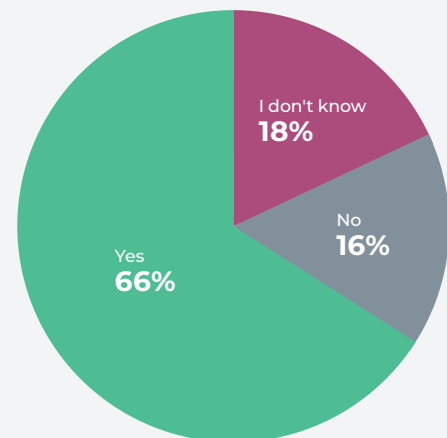
Cyber insurance is primarily intended for organizations that collect customer data and/or process credit card payments.

When you apply for insurance, the agent may ask about your security standards and their maintenance. Some companies even offer discounts to organizations that require employees to participate in ongoing security awareness programs.

66% of our respondents indicated they have cybersecurity insurance, but that doesn't mean they're in the clear.

Associations that have informal or inconsistent IT security policies risk denial on their insurance claims.

Does your organization have cybersecurity insurance coverage?



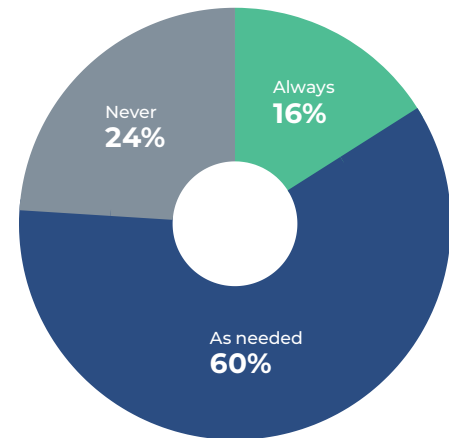
Employee Acknowledgment Forms

Over 92% of associations use employee acknowledgment forms during employee on-boarding and/if policies change, but 8% do not use them at all.

And that's a problem. A big one.

When combined with employee acknowledgment, documented policies make it far easier for human resources to take appropriate action when behavior is not in alignment. They also can be used to negotiate insurance discounts, demonstrate consistent policy enforcement, and increase chances of coverage after data breaches.

Do you require employees to sign an Employee Acknowledgment Form?



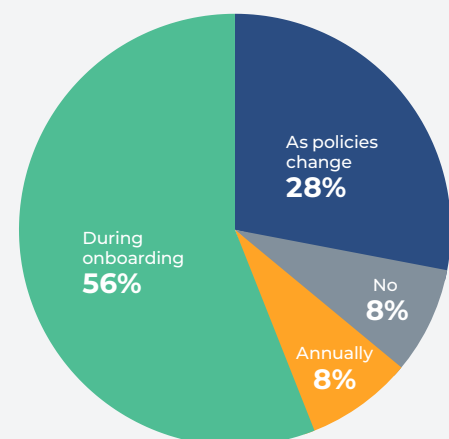
Internal Audits

In an increasingly complex world, internal audits must be conducted regularly and reported to management, but since many associations employ only a few IT personnel, external resources may be required to conduct a cybersecurity audit.

But what policies lend themselves to periodic internal audits?

- ✓ Participation and completion of employee security awareness training
- ✓ User Network Access and Permissions
- ✓ Records retention
- ✓ Personal data protection
- ✓ Data processing agreements

Do you conduct internal audits for compliance with IT policies?



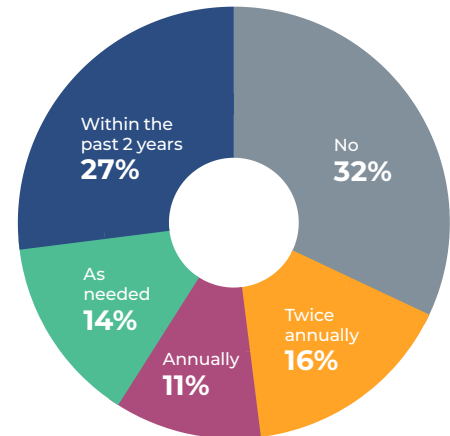
Vulnerability Testing

During a vulnerability test, your IT team or an outside expert will examine and determine which infrastructure weaknesses are in danger of exploitation.

Vulnerability tests are strongly recommended for all organizations that still maintain network infrastructure and servers on premise. Organizations that make use of private data centers or cloud hosting facilities should review ongoing audit reports on said facilities and the security practices of the companies managing those systems.

Our survey indicated that **32% of organizations do not conduct vulnerability tests on a regular basis.**

Does you conduct vulnerability testing on a regular basis?



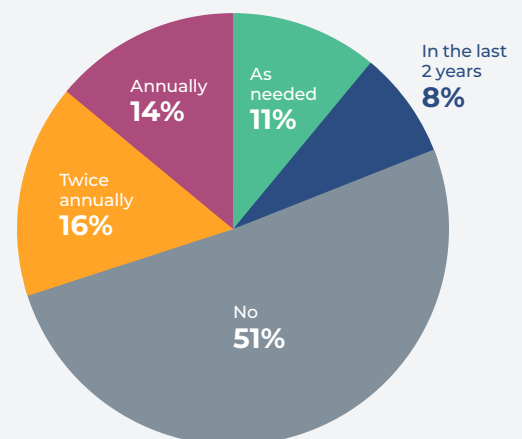
Cybersecurity Insurance

Penetration tests involve hiring a 'white-hat' hacker or firm to attempt to breach your security systems. This brings to light potential access points and weaknesses in your infrastructure that may provide opportunity for a breach. This type of assessment is conducted from outside the network as it attempts to access resources inside.

Penetration testing is required quarterly to meet PCI compliance standards, even for organizations processing less than 20,000 annual credit card payments.

Our survey reported that **51% of organizations do not participate in penetration testing.**

Do you participate in regular penetration testing?





Key Takeaways

1

Organizations across the board struggle to consistently apply formal policies. This trend is most evident in retention and email.

2

Most organizations have informal policies that remain undocumented, making enforcement extremely difficult

3

Greater than 85% of organizations report utilizing formal policies in several key areas, such as backups, network access, authentication, remote access, and passwords.

4

39% of organizations report no use of a data processing agreement policy (formal or informal).

5

50% or more of organizations report lacking formal policies in critical areas, such as outsourcing, incident response, external connection, guest access, and data processing agreements.

6

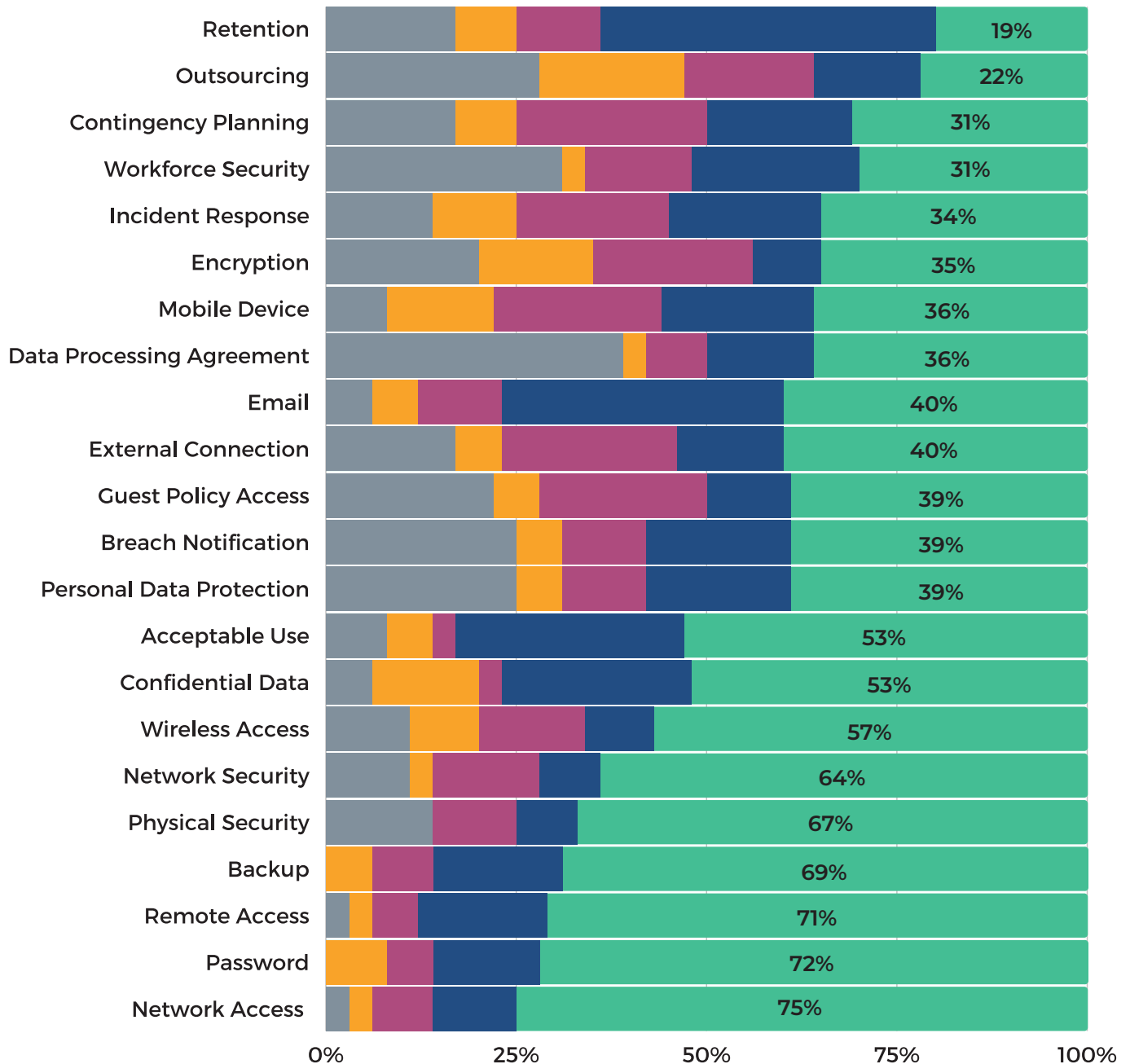
All organizations reported having remote and network access and authentication policies.

7

66% of organizations have obtained security cyber risk insurance but fail to meet the best practices to conduct IT Risk Assessment, Penetration Testing, and/or Cybersecurity Training annually.



Survey Results: Graphed



KEY

- Formal policy in place, consistently applied
- Formal policy in place, inconsistently applied
- Informal policy in place, consistently applied
- Informal policy in place, inconsistently applied
- Not in place / I'm not sure



Best Practices

Q. How often should security awareness training provided for existing staff?

A. Annually.

Q. Should associations be regularly conducting phishing tests for employees?

A. Yes. We recommend testing quarterly.

Q. How regularly should organizations conduct IT risk assessments?

A. Annually.

Q. As a smaller association, do I really need cybersecurity insurance coverage?

A. Yes. Make sure all policies are formal and reinforce underwriting in your insurance coverages.

Q. When should employees sign an acknowledgment form agreeing to abide by policies?

A. Best practice suggests providing said forms at on-boarding, after significant policy changes, and at the start of a new year.

Q. When is the best time to conduct an internal audit for IT policy compliance?

A. Annually.

Q. How often should an associations participate in penetration testing?

A. Test quarterly for PCI. If your association has no e-commerce exposures, you can test annually instead.

Q. Should associations conduct vulnerability testing on a regular basis?

A. Yes. We recommend testing annually for owned infrastructure, as well as an annual audit by outsource providers.



Policies Defined

Remote Access

Provided to define standards for accessing corporate information technology resources from outside the network, remote access policies cover all employees, contractors, and external parties that access company resources over a third-party network, whether access is performed with non- or company-provided equipment.

Password

Password policies specify guidelines for use of passwords. This policy applies to every person provided an account on the organization's network or systems, including employees, guests, contractors, partners, vendors, etc.

Confidential Data

This policy defines standards for the classification and use of confidential data, as well as specific security controls to protect said data.

The scope covers all company confidential data, regardless of location, as well as hard copies.

Mobile Device

Applicable to company data as it relates to devices that store data (i.e. laptops, notebooks, tablets, smartphones, and USB drives), this policy is used to specify company standards for the use and security of mobile devices.

Since the policy covers the data itself, ownership of the device is irrelevant.

Acceptable Use

The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

The scope includes any and all use of corporate information resources, including, but not limited to, computer systems, email, networks, and corporate Internet connections.

Retention

Retention policies specify company guidelines for retaining different types of data.

The scope covers all company data stored on company-owned, leased, or otherwise provided systems and media, regardless of location.

Email

Outlining expectations for appropriate, safe, and effective email use, this policy helps companies reduce risk of email-related security incidents, foster good business communications, and provide consistent and professional application of email principles.

Access and Authentication

This policy describes what steps must be taken to ensure users connecting to the corporate network are authenticated in an appropriate manner and are given the least amount of access required to perform their job function.

The scope includes all users with access to company equipment or access to the corporate network and/or systems.



Backup

Backup policies provide a framework to apply the backup process (read: ensuring backups are available and useful when needed).

The policy covers the type of data, frequency, storage, retention, and restoration of backups.

Outsourcing

This policy specifies actions to take when selecting a provider of outsourced IT services, provider communication standards, and protective contractual terms.

External Connection

Detailing standards for site-to-site VPNs and other external network connections, this policy specifies the security standards required for such access, ensures the integrity of data transmitted, and secures pathways into the network.

Incident Reports

Incident response policies detail exactly what must occur if an incident is suspected, covering both electronic and physical security incidents.

This policy is not intended to provide a substitute for legal advice as it approaches the topic from an IT security practices perspective.

Guest

This policy outlines procedures for securing guest access when providing network access as a courtesy to nonemployees.

The scope includes any visitor to the company wishing to access the network or Internet through company infrastructure.

Encryption

Outlining standards for the use of encryption technology, this policy ensures that encryption is used securely and managed appropriately.

It covers all data stored on or transmitted across all corporate systems.

Wireless Access

This policy states the standards for wireless access to company networks.

It covers anyone with wireless access to the network, as well as access points, routers, interface cards, and anything else capable of transmitting wireless signals.

Network Security

Network security policies establish technical guidelines for IT security and secure network infrastructure.

This policy covers all IT systems and devices comprising the corporate network.

Contingency Planning

Enabling recovery of critical IT systems, operations, and data after a disruption, contingency planning develops procedures in lieu of disruptive events.

The scope depends largely on the size and complexity of the company's network and processes.

Breach Notification

This policy details company actions in response to a breach discovery involving personal data. It covers both confidential and personal data used, controlled, or stored by the company.



Workforce Security

Ensuring members of the company workforce who can access personal data are properly authorized and supervised, workforce security policies cover most employees, including full-time, part-time, contractors, and other agents.

Data Processing

This policy specifies when a data processing agreement is required, what it entails, party obligations, and relationship structures.

It covers service provider relationships (read: anyone not a direct employee of the company workforce) that involve sharing and processing personal data.

Personal Data Protection

Personal data protection policies detail requirements for the protection of personal data as it relates to compliance with General Data Protection Regulation (EU) 2016/679 (GDPR).

The scope covers all company controlled data regardless of location, as well as hardcopies of company data.



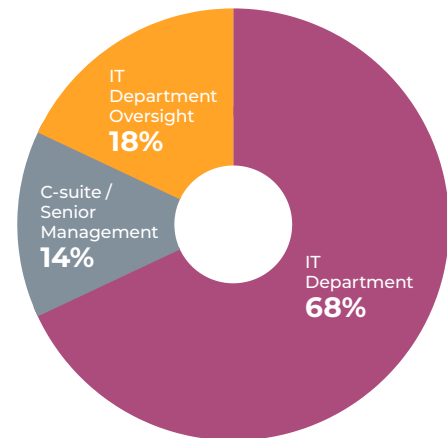
IT Security Survey: The Breakdown

Data Collection

We invited participation in 3 ways:

- 1 We sent the invitation to several groups on ASAE's online community, Collaborate. These lists included the Technology Professionals Community, the Executive Management Professionals Community, and the Finance and Business Operations Professionals Community.
- 2 We mailed the survey to our list of customers and industry colleagues.
- 3 We sent the survey announcement and link to colleagues in the association community via social media channels.

Respondent Role



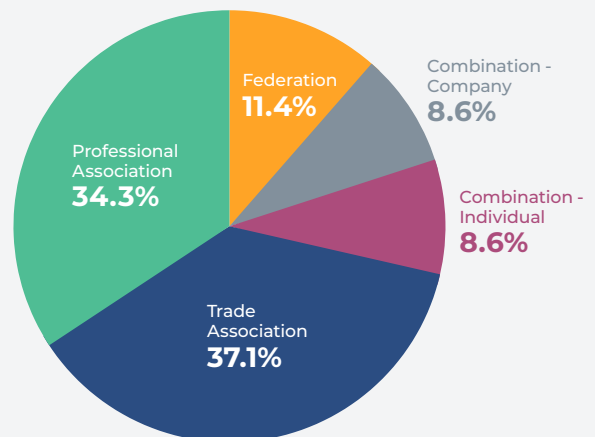
IT Staffing

The survey asked for the number of staff dedicated to IT in each organization.

- ✓ 29% indicated they had only 1 full time equivalent (FTE) in IT.
- ✓ 25.7% reported 2 or 3 FTEs.
- ✓ 3 organizations reported 0 IT staff.
- ✓ 1 organization reported 160 IT staff (which skewed the average to 8.8 FTEs).

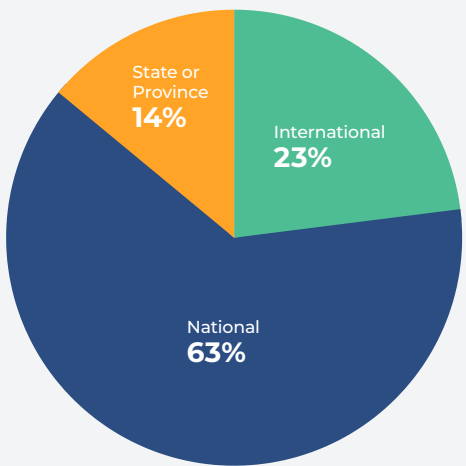
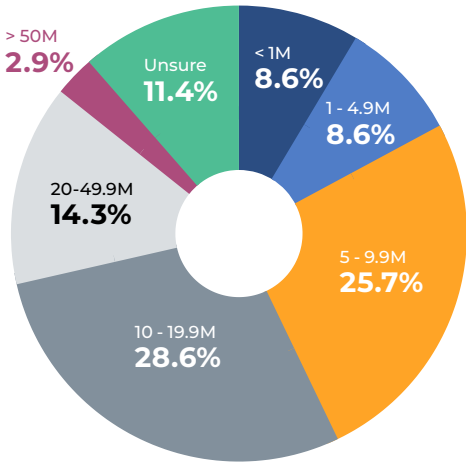
The mode was 1FTE and the mean was 3.36 FTEs.

Association Type



Annual Revenue

Survey respondents represented organizations of various sizes from <\$5M in annual revenue to up to \$50M.



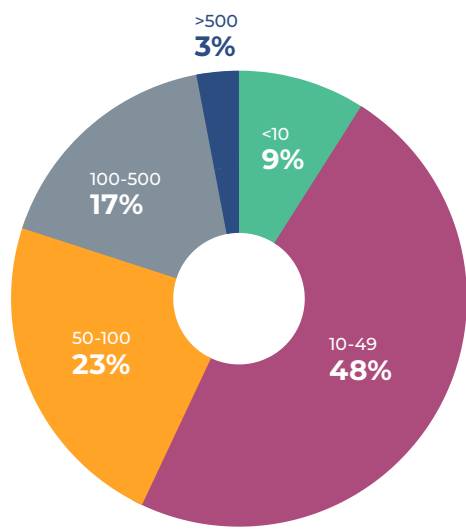
Staff Size

Respondents were from organizations of various sizes.

Scope

Respondents were from organizations of varying geographic scopes.

****None indicated they represented an organization local or regional in scope.**



About Cimatri

Remote Access

We deliver cost-effective, efficient solutions that optimize your association's technology for complete digital transformation. Our IT experts provide technology leadership, strategic planning, and IT operations oversight to ensure you are well-equipped to tackle the many challenges that come with a rapidly changing digital landscape.

Our Assessments

Technology

The key to creating a strategic IT plan and solving IT problems is understanding what technology resources you have and how they are used.

Our experienced consultants are skilled in assembling this information in a "non-techie" manner, so you can fully grasp the information presented and make the most strategic decision.

Application

Are you using the right IT business management tools?

Backed by Info-Tech industry research, our application evaluation gives you an objective view of your current tools and how they stack up. But we also take it one step further - making recommendations to improve said tools through replacement or better use processes and procedures.

Security

IT Security isn't just about penetration testing and spam filters. It's also about how people use technology.

That's why we keep a Certified Information Systems Security Professional (CISSP) on staff, so you can compare your current security practices with best practices and find your best solution for remediation.

Data Quality

Easily accessible quality data is vital for strategic decision-making. Becoming a Data-Driven Association requires that you have a solid data governance strategy.

Our consultants are experts in managing data governance challenges and will ensure you have a good program in place — and in action.

