ESG Enterprise Strategy Group | Getting to the bigger truth.™

2020 Asset Management Trends:

As IT Complexity Increases, Visibility Plummets

Dave Gruber, ESG Senior Analyst

COMMISSIONED BY

AXONIUS

CONTENTS

IT complexity is on the rise.

IT infrastructure barely resembles what it looked like just five years ago. IT transformation is driving a massive move to the cloud in all aspects of the business. The role of the data center has been diminished, with 52% of all VMs now residing in the cloud. Mobile devices are core to the operations of most business users, with an average of four devices in use by every employee, combining corporate-issued and BYOD devices. 55% of organizations indicated that they have active IoT projects, with most believing that the number of IoT devices that they support will exceed all other devices within just three years.

Together, these changes are putting enormous pressure on IT and security teams, who are already struggling to find new management and security tools that can keep up. VMs, new devices, and new device types are driving complexity. Most say that they already have too many tools, yet still report visibility gaps in what they can see versus what they want to see across cloud, mobile, and IoT environments. This gap directly translates into added security risk. 85% of organizations plan to increase investment in asset management to help overcome these issues.

52%

of all VMs now reside in the cloud.

55%

of organizations indicated that they have active IoT projects.

> *Most say that they already have too many tools, yet still report visibility gaps in what they can see versus what they want to see across cloud, mobile, and IoT environments."*

85%

of organizations plan to increase investment in asset management.

THE CLOUD TIPPING POINT

Container usage is mainstream among cloud users.

+

Growth is expected to add further complexity.

+

Organizations struggle to maintain visibility.

69%

of organizations admit that they have a **cloud visibility gap.**

75%

experienced several **serious cloud VM security incidents.**

Cloud visibility:

Hazy at best

We’re in the thick of rapid cloud adoption. VMs have reached a cloud tipping point, with 52% of VMs now residing in the cloud (on average, among cloud users). Container usage is mainstream among cloud users, with continued predicted growth that is expected to add further complexity.

With VMs running in multiple cloud environments and on-prem tools failing to deliver multi-cloud management options, organizations struggle to maintain visibility and manage VMs effectively.

Cloud visibility gaps are prevalent, with 69% of organizations admitting that there is a cloud visibility gap between what they can see and what they want to see when it comes to cloud-hosted VMs, to 75% experiencing several serious cloud VM security incidents.

End-user devices:

Our end-users have devices. We know that much.

73% of organizations admit to having an end-user device visibility gap, citing lack of inventory and activity visibility, while 73% cop to experiencing multiple, serious incidents, like data breaches involving end-user devices.

73%

admit to having an end-user device visibility gap.

73%

admit to experiencing multiple, serious incidents.

40%

On average, organizations think they're blind to around 40% of devices with issues.

> *Security incidents are directly related to visibility gaps."*

2.3x

Those organizations with the most problematic visibility **are experiencing twice as many incidents.**

Respondents report that managing different device types requires multiple tools and that **keeping up with usage growth is a challenge.**

Back to Contents

49%
of organizations prohibit BYOD use for work-related activities.

61%
of those that have BYOD policies are concerned they are being violated.

> *“BYOD looks to be here to stay....*
> ***even if security suspects that policies are being circumvented.”***

A typical employee uses
more than 4 devices each week.

Bring your own device:

BYOD, CYA, and trust - isn’t this 2020?

15+ years after the term was coined, we’re still talking about bring-your-own-device (BYOD) policies and how they relate to security. The survey revealed that nearly half (49%) of organizations prohibit BYOD use for work-related activities, but 61% of those that have BYOD policies are concerned they are being violated.

And with a typical employee using more than 4 devices each week, BYOD looks to be here to stay....even if security suspects that policies are being circumvented.

BYOD creates a trust issue. Even when companies don’t own a device, they do own securing company assets accessed from that device. Without ownership, can IT and security teams effectively inventory, manage, and secure them?

Back to Contents

The IoT explosion:

IoT is “inevitable or terrifying.”

We’re still in the nascent days of IoT and most are still preparing for the IoT inevitability. By some reports, there will be 500 billion connected devices by 2030 (Cisco). Looking to the future, 81% feel that IoT devices will outnumber all other devices within 3 years, but less than half are confident in their IoT visibility strategy.

IoT is definitely happening, with 55% of organizations reporting active IoT projects, but most are concerned about visibility, with 77% reporting a visibility gap.

With a wide array of IoT device types, gaining the visibility and control needed is challenging, with 58% reporting that the diversity in device types is among their biggest management challenges.

Respondents are evenly split as to whether they believe they have a solid strategy for gaining visibility into IoT devices. While 55% of organizations already have IoT initiatives underway, 47% report feeling confident in their visibility strategy for those devices. Yet another 46% say they are uncertain about visibility, as they plan their IoT initiatives. Uncertainty in visibility strategies is unacceptable!

81%

feel that IoT devices will **outnumber all other devices within 3 years.**

55% of organizations report active IoT projects.

Concerns remain, with **77%** reporting a visibility gap.

58% say diversity in devices is their biggest management challenge.

LOOKING TO THE FUTURE

47%

report feeling **confident** in their visibility strategy for those devices.

46%

say they are **uncertain** about visibility.

Back to Contents

On average, organizations are using

108 separate security tools.

> Asset inventories are *overwhelmingly complicated!*

IT ASSET INVENTORIES

Require **89** person-hours of labor.

+

Happen **19** times per year.

+

Demand the involvement of **multiple** teams.

Challenges:

Visibility and security

Securing all of this is a nightmare to manage. Even with the use of over 100 separate security tools, on average, organizations still report visibility gaps. Security complexity (threats, regulations, etc.) drives more siloed tools investment, further complicating the problem.

And it will become even more unmanageable, unless we solve the first problem: understanding and managing what we have.

Asset inventories are overwhelmingly complicated! Comprehensive IT asset inventories take over 2 weeks of effort (89 person-hours of labor) and happen 19 times per year, on average, requiring multiple teams and people. A new approach is needed.

IT and security teams want more.

The rapid pace of infrastructure change will continue to add complexity, adding new device and workload types that further increase the attack surface. Lack of visibility exposes organizations to new threats and compliance issues.

IT and security teams want more visibility than they currently have. Yet the process to acquire this visibility is both time-consuming and resource-intensive, and produces incomplete and out-of-date results as soon as it is finished. IT and security teams can no longer afford both the resource drain and the time-to-result delays -- especially when these visibility gaps correlate to an increase in security incidents.

Any time spent on manual asset management tasks is taking precious time away from already stretched security resources. When asked what they would do if they could free up resources from asset-related tasks, roughly 90% said they would see a material impact, using that time for things like proactive threat hunting and more thorough incident response investigations.

To combat the present, growing, and future visibility issues, 85% of organizations say they will increase investment in asset management in the next 24 months.

Investing in a cross-platform, cross-device, hybrid-cloud enabled asset visibility solution eliminates multiple existing tools, closes IT and security gaps, and frees up critical resources to focus on other priority initiatives.

> *“IT and security teams can no longer afford both the resource drain and the time-to-result delays.”*

A MATERIAL IMPACT

~90%

expect the time freed up from asset-related tasks would have a material improvement on threat hunting and incident investigations.

85%

of organizations say they will increase investment in asset management in the next 24 months.

Back to Contents

AXONIUS

Axonius can help.

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with over 200 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately. Covering millions of devices at customers like the New York Times, Schneider Electric, Landmark Health, AppsFlyer, and many more, Axonius was named the Most Innovative Startup of 2019 at the prestigious RSAC Innovation Sandbox and was named to the CNBC Upstart 100 list and Forbes 20 Rising Stars. For more, visit Axonius.com.

Request a Demo

About ESG

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

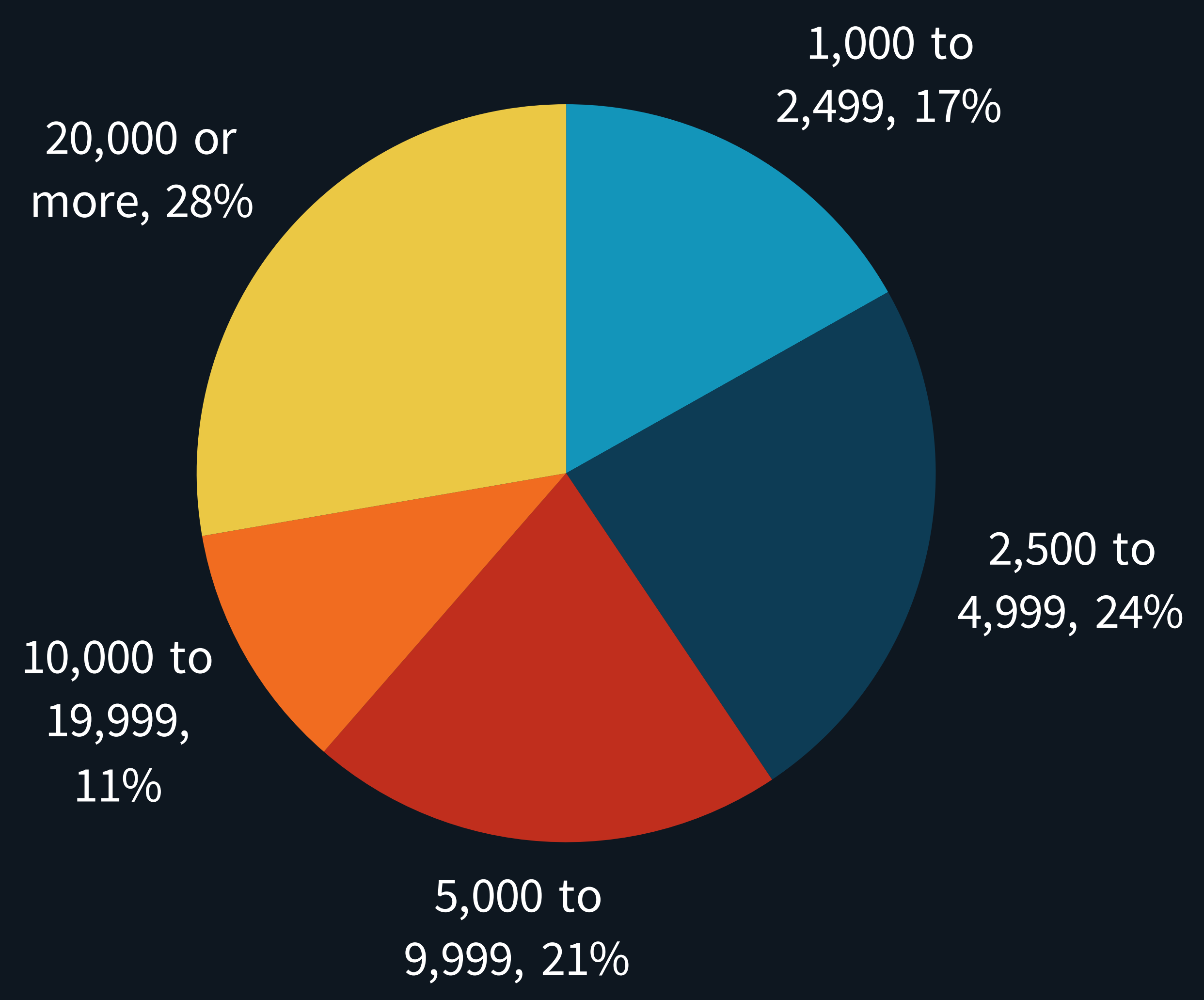
Back to Contents

Research Methodology

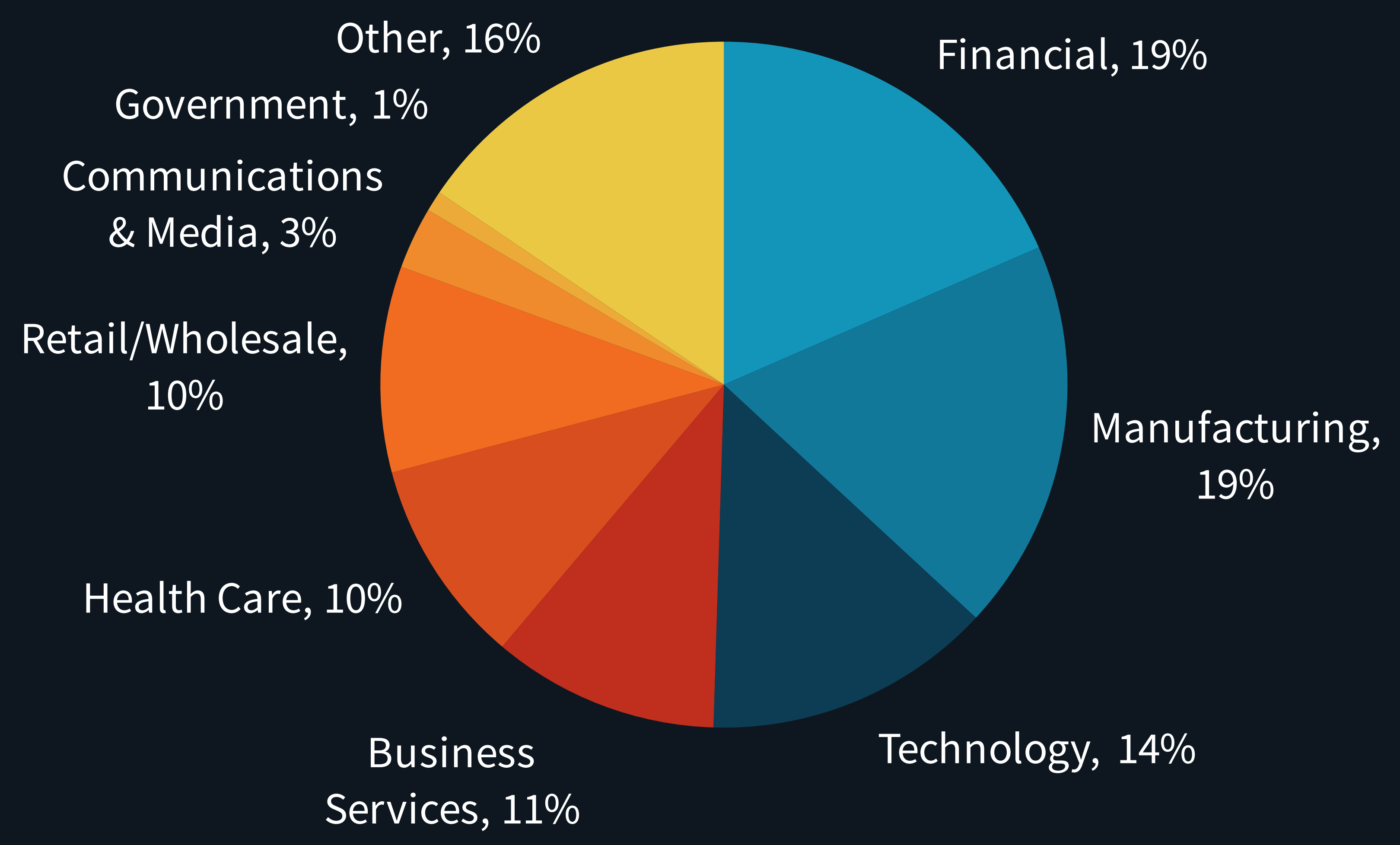
To gather data for this eBook, ESG conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America (United States and Canada) between December 6, 2019 and December 21, 2019. To qualify for this survey, respondents were required to be IT or cybersecurity professionals personally knowledgeable with their organization's cybersecurity environment and cloud infrastructure usage. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 200 IT and cybersecurity professionals.

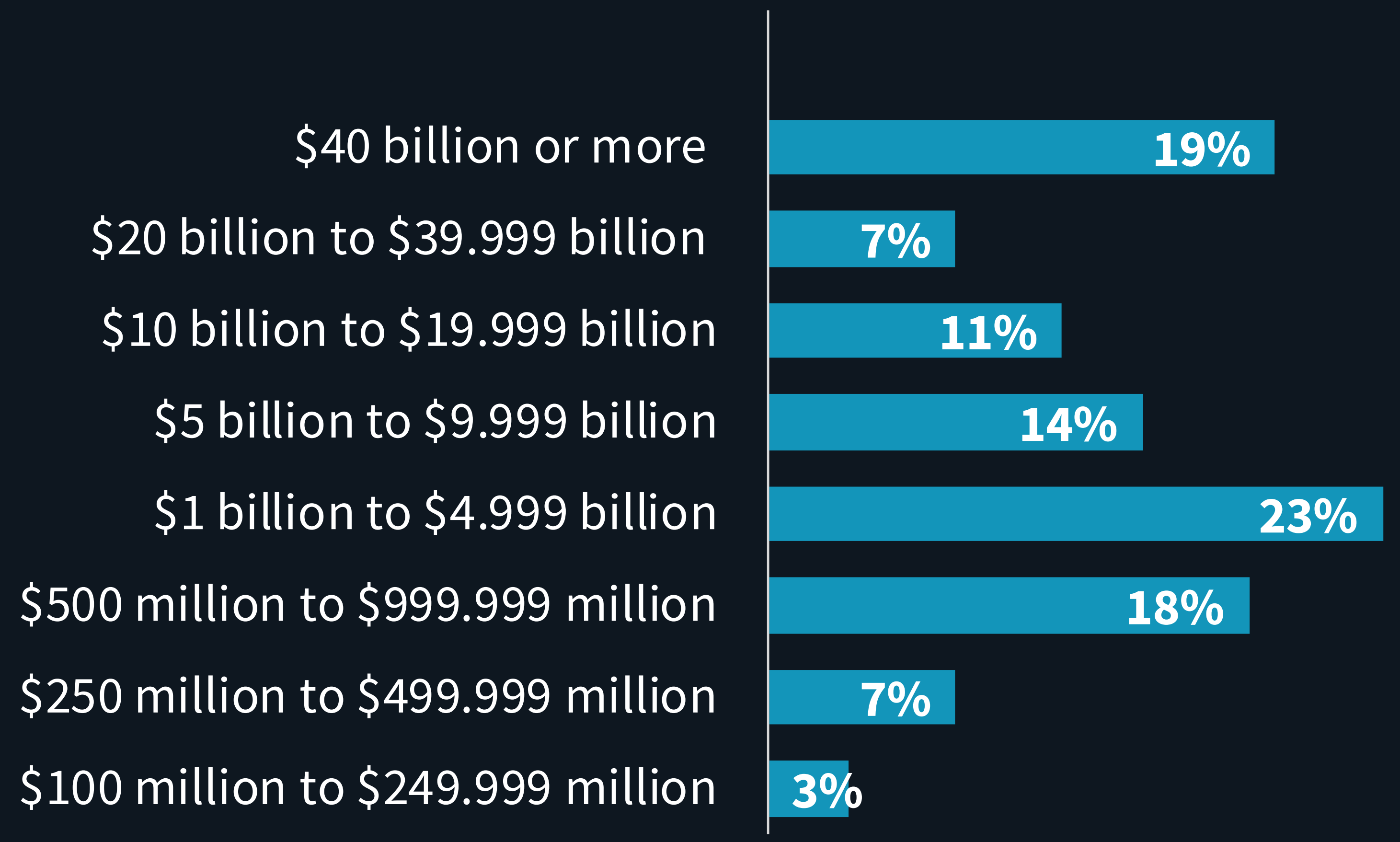
RESPONDENTS BY NUMBER OF EMPLOYEES



RESPONDENTS BY INDUSTRY



RESPONDENTS BY REVENUE



Back to Contents

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides actionable insight and intelligence to the global IT community.