# CYBERSECURITY FRAMEWORKS AND FOUNDATIONAL SECURITY CONTROLS

## A SURVEY OF IT SECURITY PROFESSIONALS

November 2016

dimensional research

Sponsored by

Center for Internet Security

tenable network security

# CYBERSECURITY FRAMEWORKS AND FOUNDATIONAL SECURITY CONTROLS

## A SURVEY OF IT SECURITY PROFESSIONALS

Dimensional Research | November 2016

## Introduction

Foundational security controls, common to virtually all security frameworks, serve as an important starting place to achieve cybersecurity effectiveness and efficiency. These security controls serve as a solid foundation for subsequent controls. If these foundational security controls are not implemented correctly, investments in subsequent incident detection and response controls will be less effective, and the overall cybersecurity framework objectives will not be met. So where are today's organizations on their cybersecurity framework journey? And what is the status and maturity of foundational security controls within this journey?

The following report, sponsored jointly by Tenable Network Security and the Center for Internet Security, is based on a survey of 319 IT security decision makers at companies with more than 100 employees. The goal of the survey was to quantify adoption and maturity of cybersecurity frameworks and their underlying foundational security controls.

## Key Findings

- **Security teams are on a framework adoption journey**
  - 80% use a security framework today
  - Less than half (44%) have used security frameworks for more than 12 months
- **Adoption of frameworks have clear benefits**
  - 95% have seen benefits from framework adoption
  - Certain benefits are achieved quickly, but some take time
  - Those who adopted a framework more than 12 months ago are more likely to be positive about their overall security program
- **Many challenges are faced when implementing frameworks**
  - 95% have faced impediments with implementation of their framework
  - Issues are both organizational and technological
- **Increased focus on foundational controls is clearly needed**
  - Foundational controls are not widely implemented
  - 44% have automated less than 1/3 of the foundational subcontrols
  - The typical company (50th percentile) has automated only 6 of 15 foundational subcontrols

dimensional research

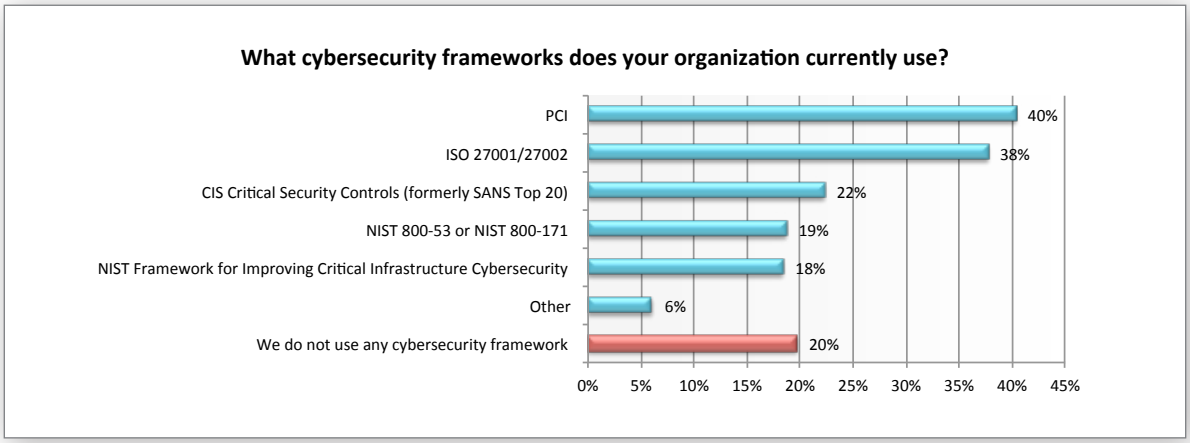
Sponsored by Center for Internet Security

tenable network security

# Detailed Findings

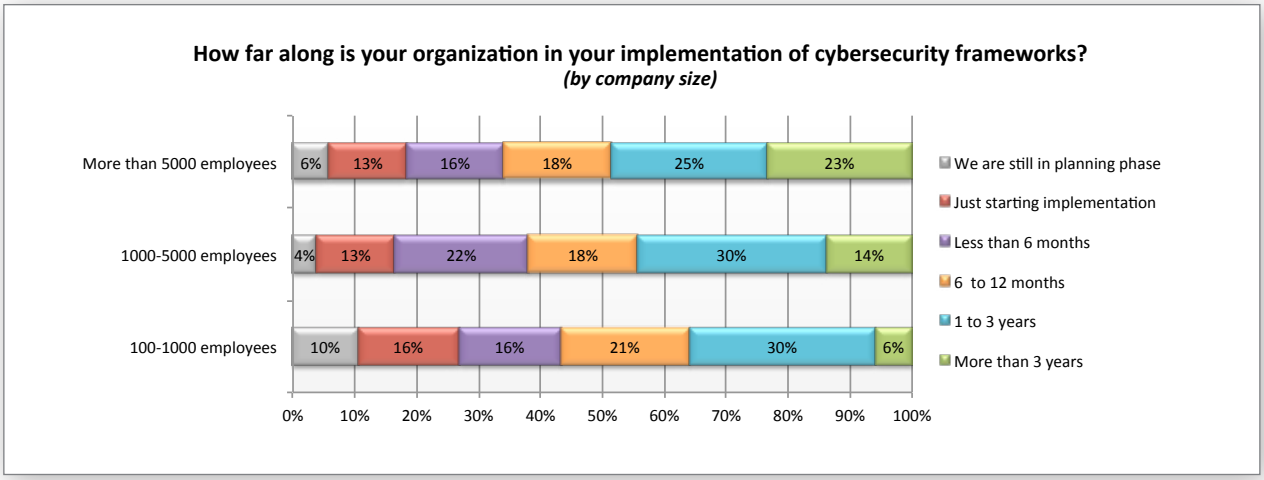
## Security teams are on a framework adoption journey

Today's security teams are looking for all the help they can get to do an increasingly difficult job. Frameworks have become a common place to look for guidance, with most companies, 80%, saying they use a cybersecurity framework. While the specific framework chosen various widely – from PCI (40%), ISO 27001/27002 (38%), and CIS Critical Security Controls (22%) through to the National Institute of Standards and Technology (NIST) frameworks (almost 20%) as well as other frameworks such as HITRUST, DoDAF, and more – the adoption of a cybersecurity framework is common.

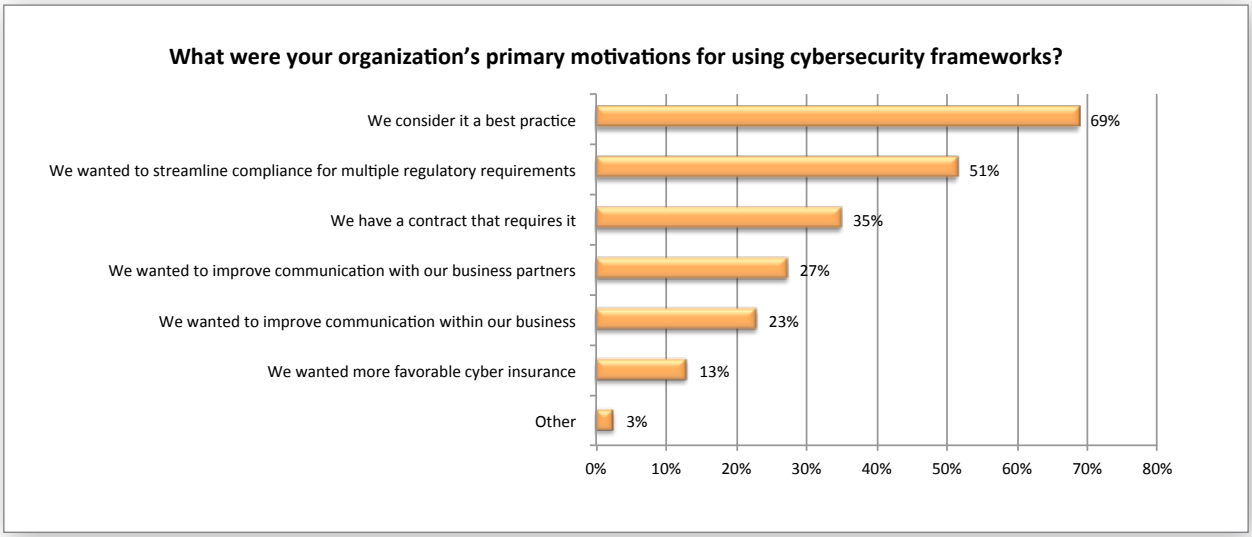



Cybersecurity framework adoption is a relatively recent move for many security teams. The framework journey is just starting for the more than half of security teams, with 56% reporting that they only began adopting their framework within the past year. This includes 20% who are at the very beginning of the journey - either still in planning phase (6%) or have having just started their implementation (14%).

Company size does have an impact on adoption of security frameworks, but a fairly minor one. Larger companies are slightly ahead in their adoption of frameworks. For example, in large companies (5000 employees or more) almost a quarter (23%) started their cybersecurity framework implementation more than 3 years ago compared to only 6% at small companies (those with 100-1000 employees). However, across all size companies we see that more than half (52% at large companies, 56% at mid-sized companies and 64% at small companies) started their framework adoption within the past year.

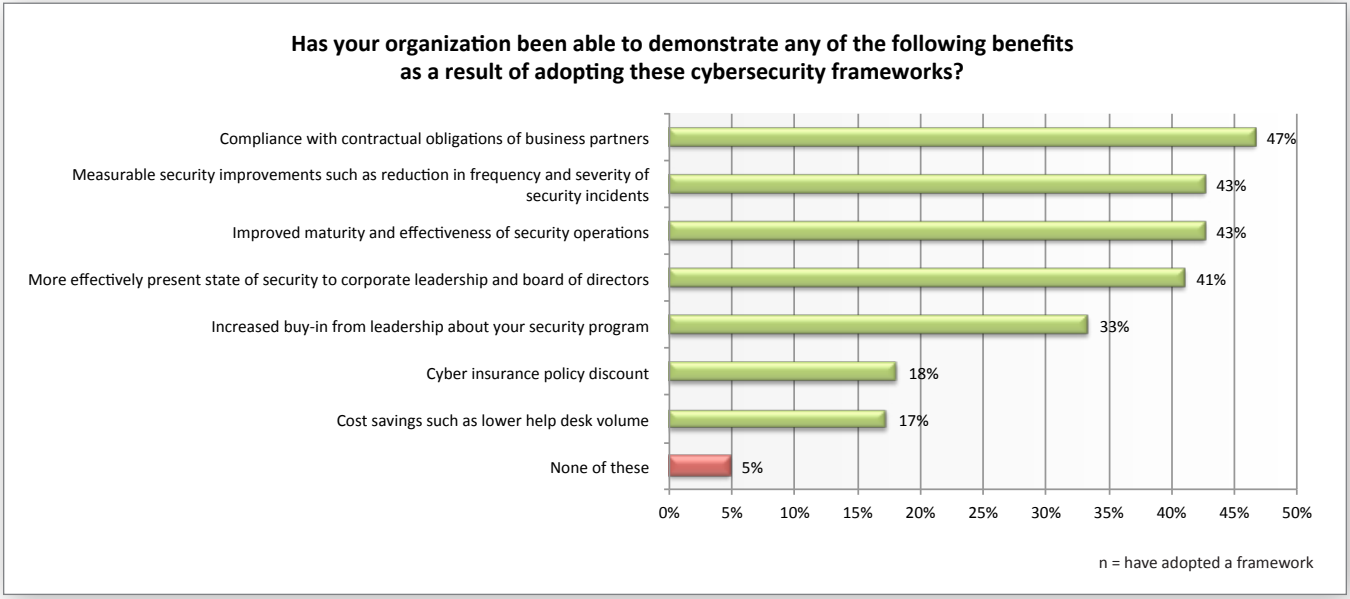



The most common motivation reported for adoption of a cyber security framework is that the framework is viewed as a best practice (69%). Other motivations ranged from streamlining compliance for regulatory requirements (51%), being contractually required (35%), and improving communication with partners (27%) or within the business (23%). Some were motivated to adopt a framework as a means of achieving more favorable cyber insurance rates (13%). Other motivations were reported including accepting credit cards or a need for guidelines for internal policies.

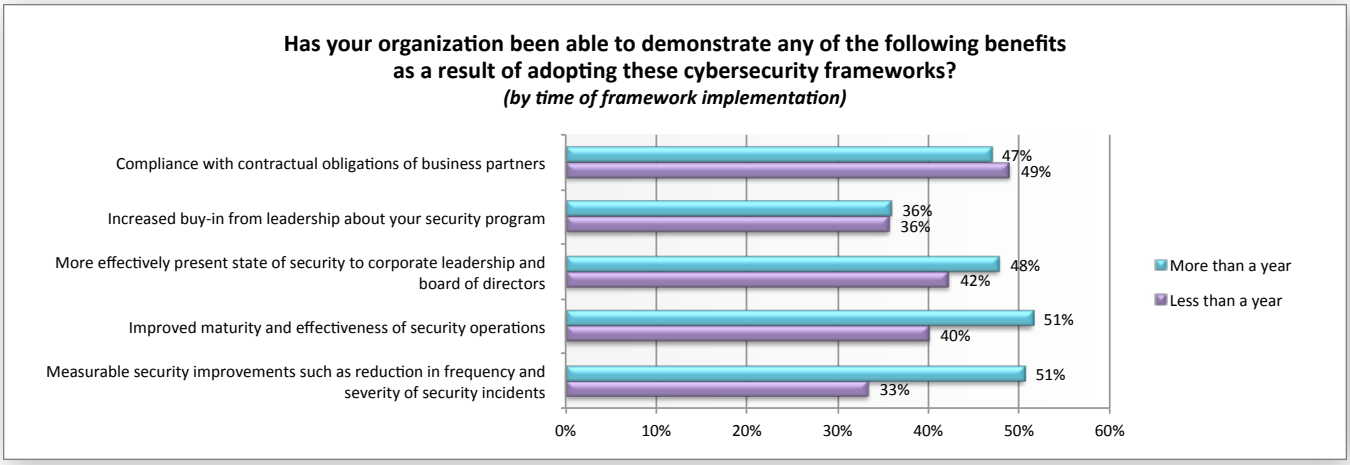


## Adoption of security frameworks delivers clear benefits

Those who do adopt security frameworks see clear benefits. The vast majority (95%) report that their organizations have benefited. Top benefits include compliance with contractual obligations (47%), achieving measurable security improvements (43%), improved maturity and effectiveness of security operations (43%), and ability to more effectively present security readiness to business leadership (41%).

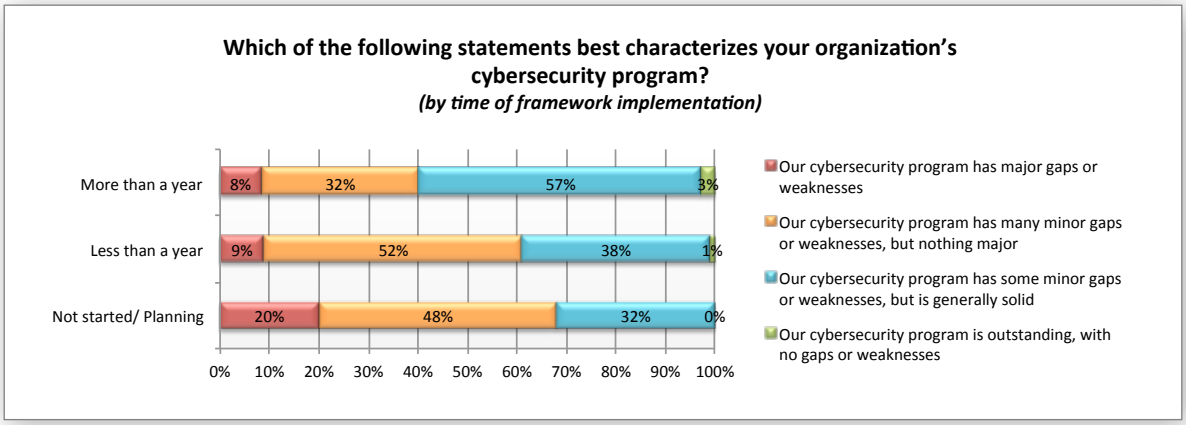



Interestingly, if you consider the experiences of those who started adopting frameworks within the past year with those who started adopting their framework over a year ago, a clear pattern emerges. Some of these benefits appear to be fairly immediate, including compliance with contractual obligations and increased buy-in from leadership, which both groups reported in about the same numbers. However, certain benefits appeared to take more time, such as the ability to present effectively to business leadership, improved maturity of security operations, and measurable security improvements. Among those who had starting implementing their framework over a year ago, significantly more companies reported achieving these benefits.



It should be noted that among the 5% that are adopting security frameworks but haven't seen benefits, the most common reason (more than half) is simply because it is too soon to see results. Across the entire survey, only 2 individuals (less than 1%) reported that they felt that they did not see benefits because the framework itself was not effective.

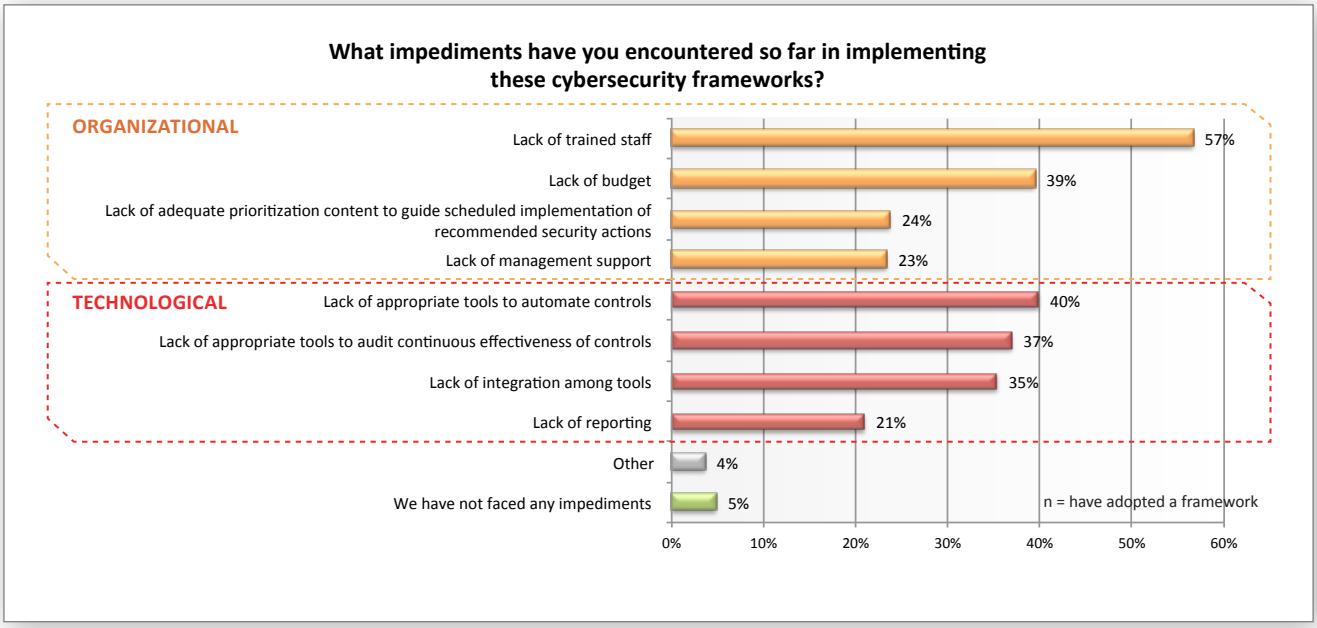
There is a correlation between the maturity of cybersecurity framework adoption and confidence in the overall cybersecurity program. Among those who started adopting their cybersecurity framework over a year ago, 60% were confident about their cybersecurity program compared to only 32% of those who have not started or are in the planning phase with their cybersecurity framework.




## Significant challenges are faced when implementing frameworks

Adoption of cybersecurity frameworks is not without challenges. Almost all (95%) of those who have adopted a framework have faced impediments.

The issues reported included organizational issues such as lack of trained staff (57%), inadequate budget (39%), lack of prioritization (24%), and not enough management support (23%). There were also technological issues including lack of appropriate tools to automate controls (40%), inadequate tools to audit effectiveness (37%), poor integration between tools (35%), and lack of reporting (21%). Other challenges reported included not having enough time and conflicts between usability and security needs.




## Foundational controls are not widely implemented

Foundational security controls are common to virtually all frameworks. To gain a deeper understanding of the status of the framework journey, we asked specific questions about implementation of certain foundational controls.

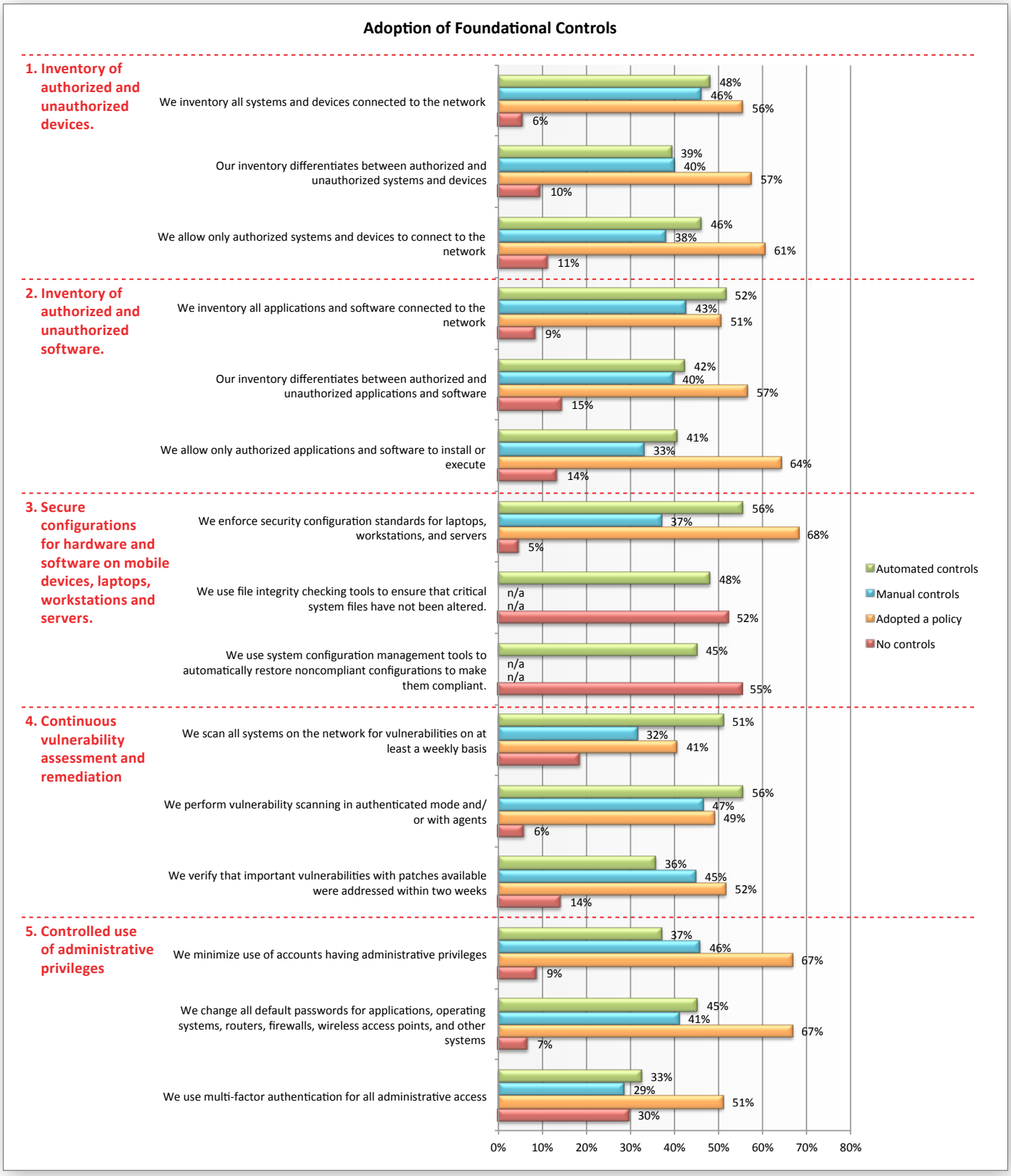
This research focused on the Foundational Cyber Hygiene controls identified by the Center for Internet Security (CIS) as being the most fundamental and valuable actions that every enterprise should take. According to the CIS:

"Foundational Cyber Hygiene controls are basic things you must do to create a strong foundation for your defense. This is the approach taken, for example, by the DHS Continuous Diagnostic and Mitigation (CDM) Program, one of the partners in the CIS Critical Security Controls. A similar approach is recommended by our partners in the Australian Signals Directorate (ASD) with their 'Top Four Strategies to Mitigate Targeted Intrusions.[1]'"

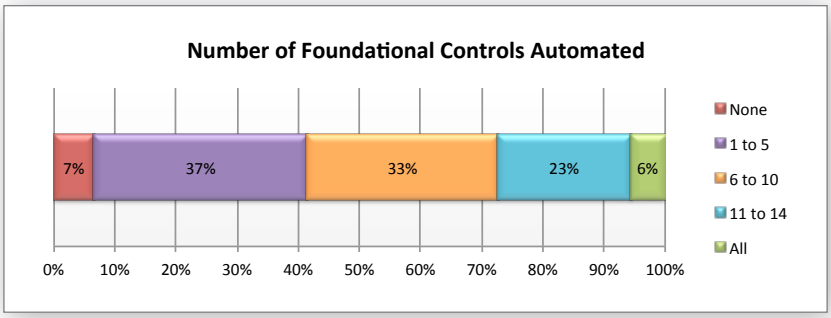
We selected 3 subcontrols with increasing levels of maturity for each of the five Foundational Cyber Hygiene controls, for a total of 15 of the most important controls. For each of these 15 controls, we asked about the types of controls in place – automated, manual, policy, or no controls.

A clear picture emerged. While most do have foundational controls in place, there is still a strong reliance on policies and manual controls.

1 Center for Internet Security, "The CIS Critical Security Controls for Effective Cyber Defense v6.1", 2016

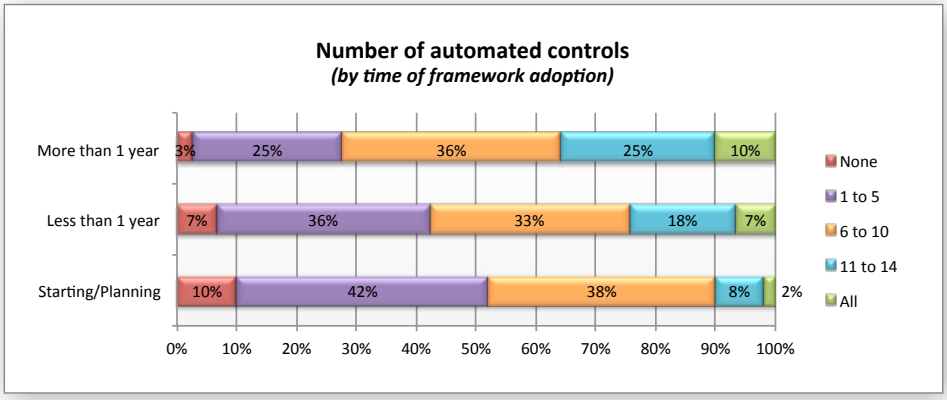


Automated controls are ideal, but they are still not the norm. Across the 15 subcontrols studied, only low levels of automation were seen. The typical company (the 50th percentile), has automated only 6 of these 15 subcontrols. Even at the top companies (the 80th percentile) only 11 of these 15 controls have been automated.




Only 6% have automated all 15 of these foundational security subcontrols. There were some clear trends among companies who had automated all subcontrols. Half of these (50%) were from very large companies with more than 15,000 employees. More than half (59%) had started adopting a cybersecurity framework more than a year ago. And more than a third (38%) worked at financial services companies. Most interestingly, almost all of them (92%) are adopting or have adopted a cybersecurity framework.

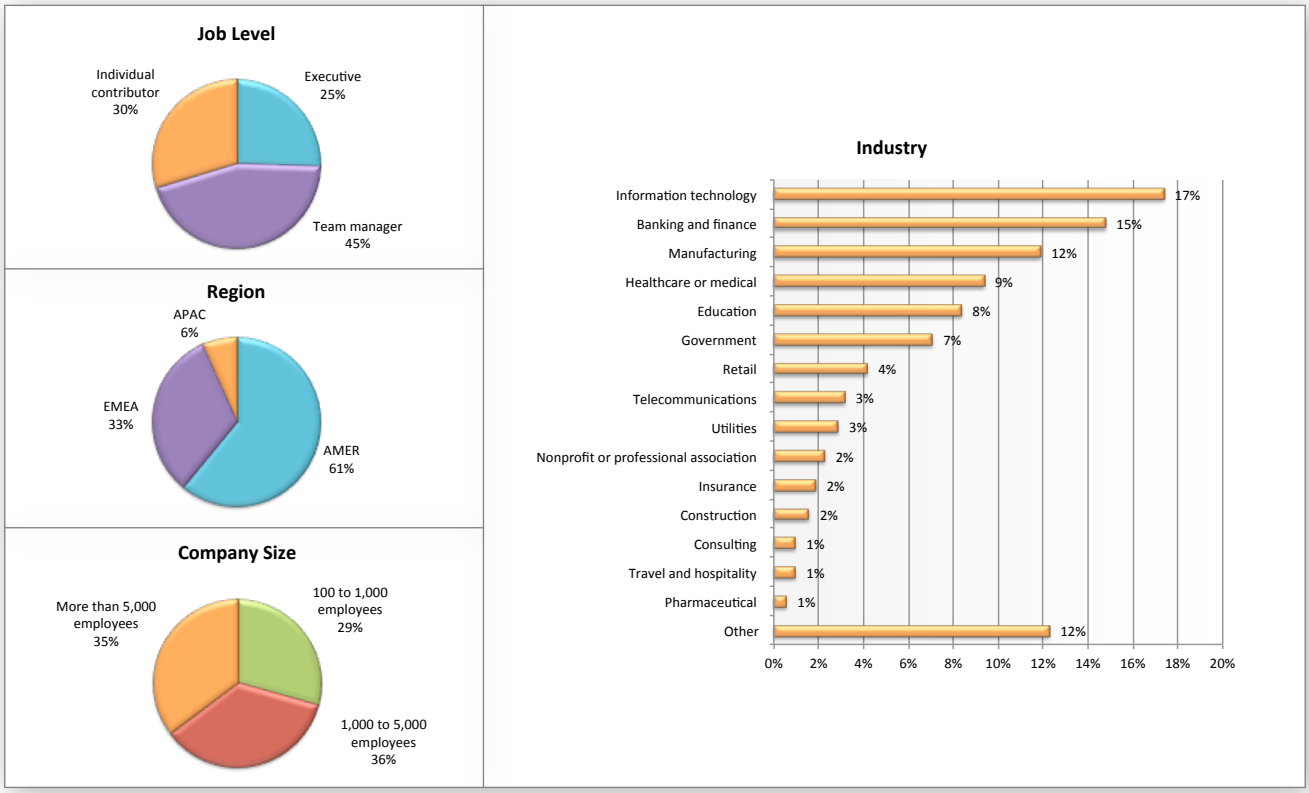
There is a clear correlation between the time a cybersecurity framework has been in place and the number of controls that have been automated. For example, among companies that started adopting a cybersecurity framework more than a year ago, 35% have automated more than 11 subcontrols compared to only 10% of those who are only in the planning phase or just beginning their implementation.



## Survey Methodology and Participant Demographics

In the fall of 2016, IT security professionals at companies with more than 100 employees were invited to participate in an online survey on the topic of the security of their data and systems. Participants were asked a series of questions about their security programs, adoption of security frameworks, and level of adoption of foundational security controls.

A total of 319 qualified participants completed the survey. All participants were security professionals at companies with more than 100 employees. A wide range of job levels, company sizes, and vertical industries were represented.





## About Dimensional Research

Dimensional Research® provides practical market research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how corporate IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. For more information, visit dimensionalresearch.com.

## About Tenable Network Security

Tenable Network Security transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring. For more information, please visit tenable.com.

## About the Center for Internet Security

The Center for Internet Security (CIS) is a 501(c)(3) organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. Utilizing its strong industry and government partnerships, CIS combats evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC), CIS Security Benchmarks, and CIS Critical Security Controls.