
TRENDS IN SECURITY FRAMEWORK ADOPTION

A SURVEY OF IT AND SECURITY PROFESSIONALS

March 2016

TRENDS IN SECURITY FRAMEWORK ADOPTION

A SURVEY OF IT AND SECURITY PROFESSIONALS



Dimensional Research | March 2016

Introduction

IT security has become a top challenge for all modern organizations. A wide range of security frameworks are available to guide companies in their efforts to protect their critical systems and data each with its own specific focus. But are security teams leveraging these frameworks? Are they focused on only one approach or combining a variety of different frameworks? How quickly are they maturing with their use?

The following report, sponsored by Tenable Network Security, is based on a survey of 338 IT and security professionals in the United States. The goal of the survey was to quantify adoption of security frameworks. Questions were asked on a wide range of topics to understand which security frameworks were adopted, motivations for adoption, and how fully they were adopted.

Security Framework Acronyms:

ISO = ISO/IEC 27001/27002

CIS = CIS Critical Security Controls

CSF = NIST Framework for Improving Critical Infrastructure Cybersecurity

PCI = Payment Card Industry Data Security Council Standard

Key Findings

- **Security frameworks guide the way**
 - 84% leverage a security framework
 - Security frameworks used by broad range of company sizes and industries
- **Wide range of security frameworks utilized**
 - 44% use more than one security framework
 - By end of 2016, adoption of CSF (43%), CIS (44%), and ISO (44%) will be similar
- **Best practice and requirements both drive CSF adoption**
 - 70% adopted CSF because they consider it a best practice
 - 29% adopted CSF because a business partner required it
 - 28% adopted CSF because a federal contract required it
- **Security framework adoption is a journey**
 - Only about 1 in 5 rank their organization as “very mature” in adoption of CSF
 - More than half of CSF adopters still require significant investment to fully conform

TRENDS IN SECURITY FRAMEWORK ADOPTION

A SURVEY OF IT AND SECURITY PROFESSIONALS

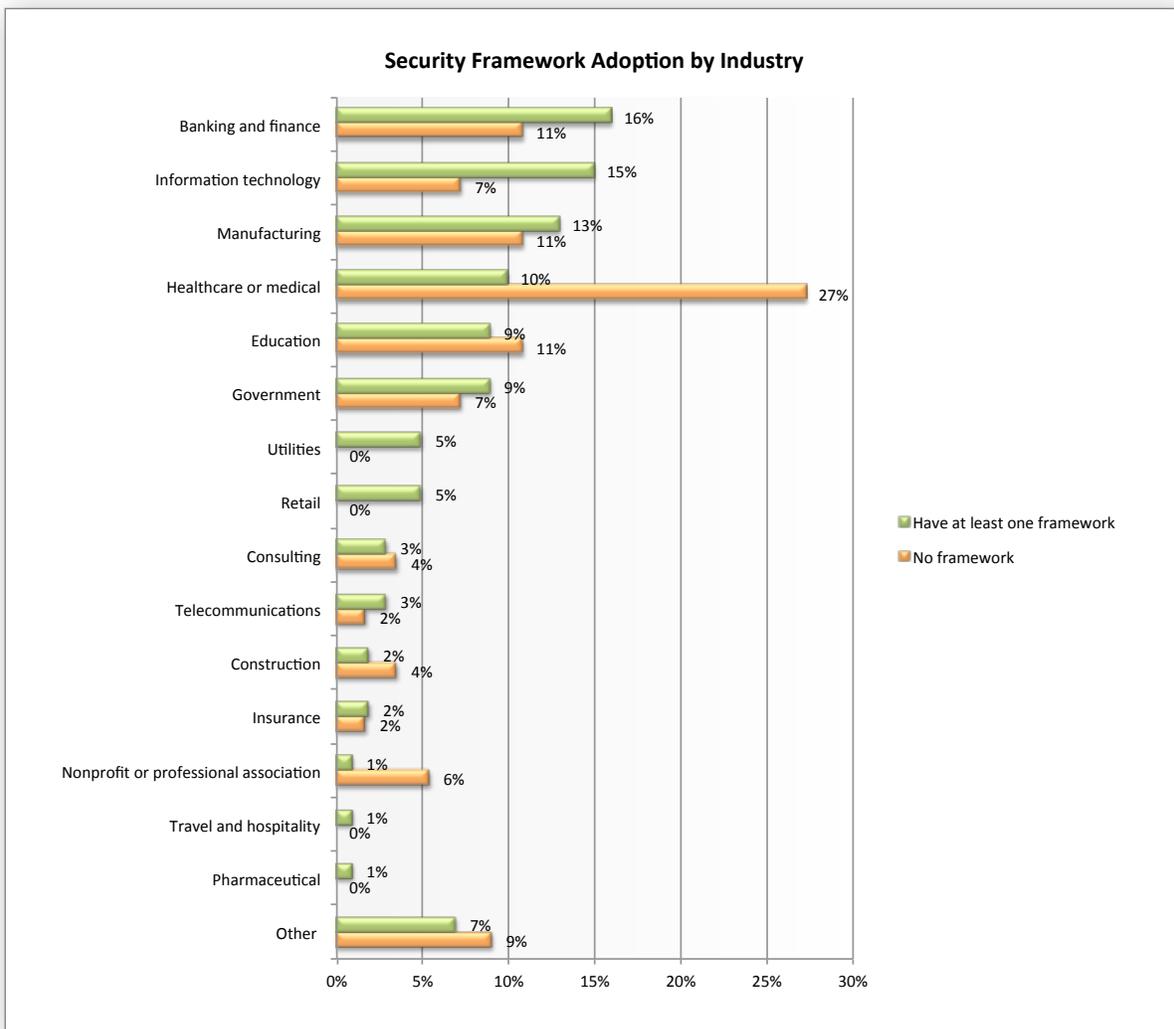


Dimensional Research | March 2016

Detailed Findings

Security frameworks are guiding the way

Keeping critical systems and data secure is a challenge that touches all types of companies. To help address these challenges, a wide range of industries are looking to security frameworks for guidance. When we look across all IT and security professionals whose companies have adopted security frameworks, we see that they represent all industries from banking to government to utilities and many more.



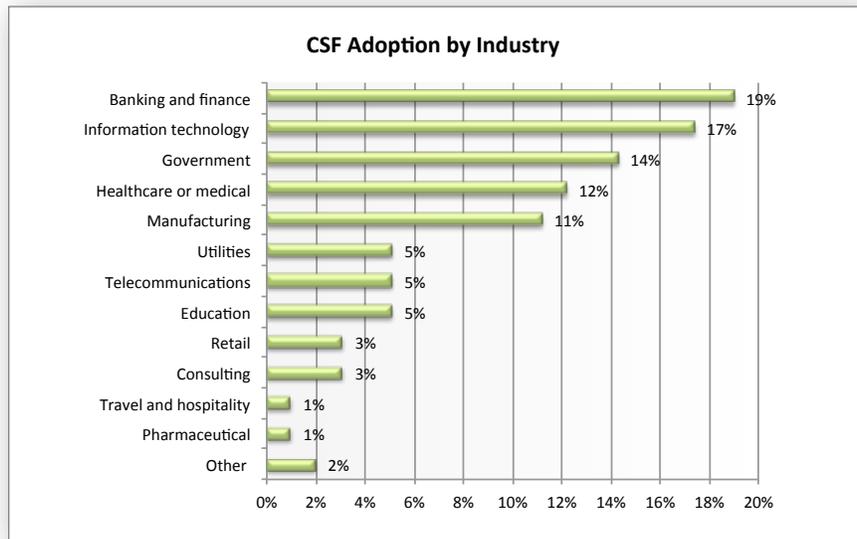
TRENDS IN SECURITY FRAMEWORK ADOPTION

A SURVEY OF IT AND SECURITY PROFESSIONALS

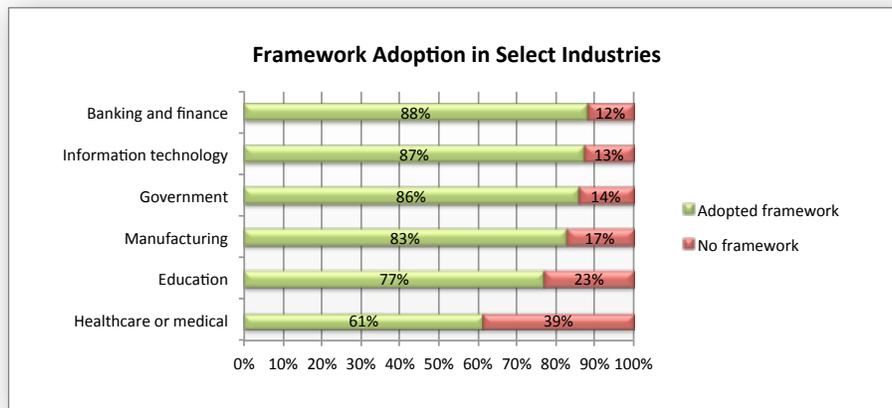


Dimensional Research | March 2016

Many security frameworks have a strong reputation in specific areas. CSF is an initiative of the United States federal government, PCI is typically connected to retail which relies on credit card transactions, and ISO is most known internationally. This research clearly shows that despite reputation, security frameworks are not limited only to specific audiences. For example, if we consider all companies that report adoption of CSF, we do see that a broad range of industries in addition to government are using CSF, including banking, healthcare, education, retail, and more.



Examining the scope of adoption for these different industries, we do see adoption of security frameworks is the norm. Considering the industries for which we have adequate participation to allow for reasonable analysis, we see banking and finance, information technology, government, and manufacturing all have security framework adoption rates above 80%. Education and healthcare follow slightly behind at 77% and 61% respectively.



TRENDS IN SECURITY FRAMEWORK ADOPTION

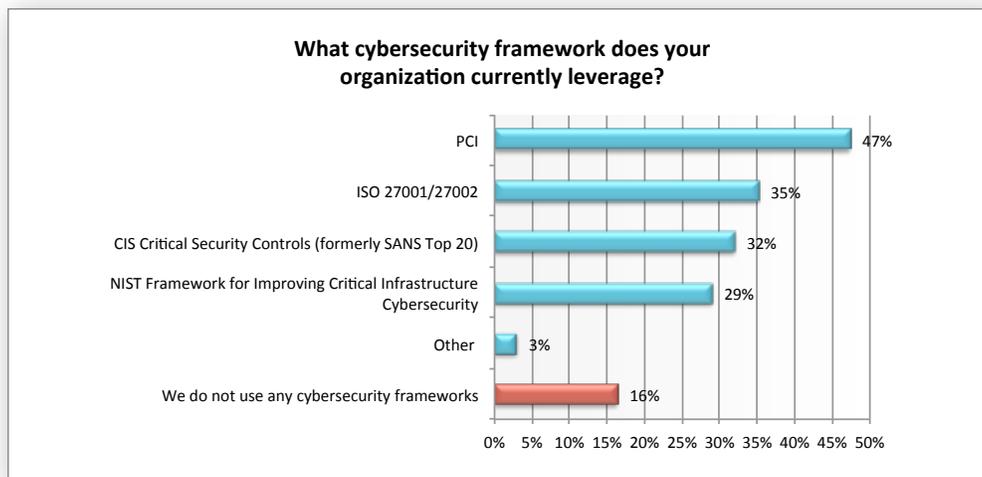
A SURVEY OF IT AND SECURITY PROFESSIONALS



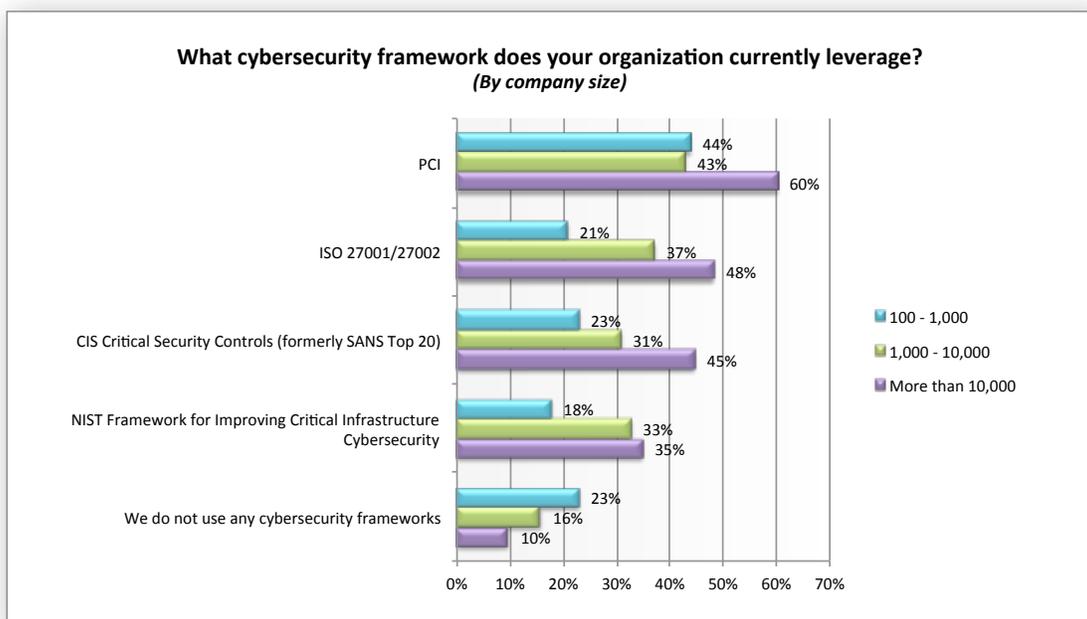
Dimensional Research | March 2016

Adoption spread across multiple leading security frameworks

Adoption of security frameworks is definitely common practice. The vast majority of companies (84%) are leveraging a security framework. There is no single security framework that is being used by the majority of companies. There are several security frameworks in common use including PCI (47%), ISO (35%), CIS (32%), and CSF (29%). The survey participants who took the time to write in “Other” answers added HIPAA, FFIEC, HITECH, CIP, and internally-developed guidelines to this list.



Security framework adoption is common across all sized companies. Companies with more than 10,000 employees are slightly more likely to have adopted a security framework (90%) but even smaller companies with less than 1,000 employees report significant rates of adoption (77%).



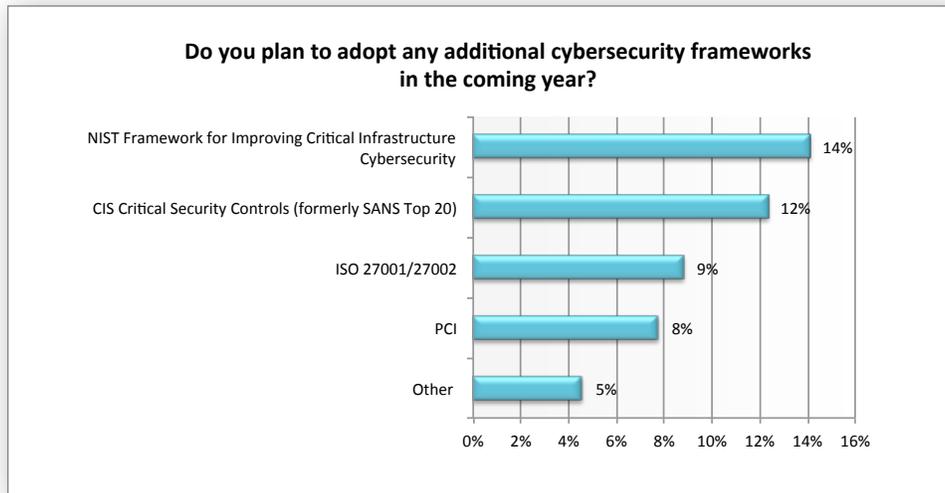
TRENDS IN SECURITY FRAMEWORK ADOPTION

A SURVEY OF IT AND SECURITY PROFESSIONALS

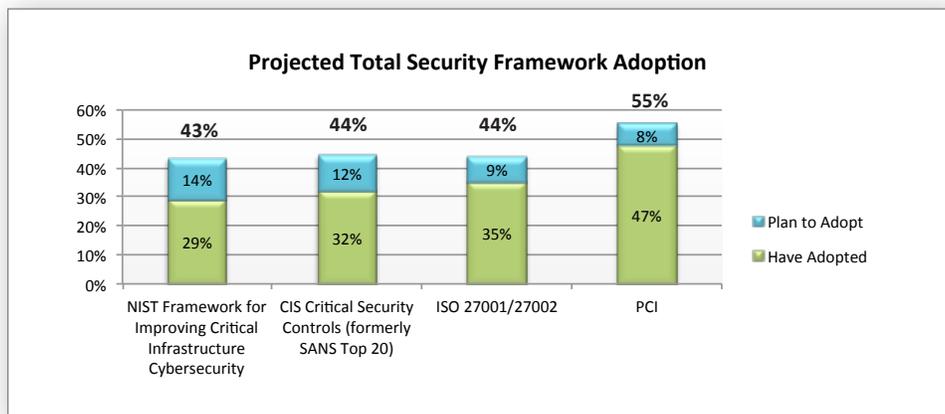


Dimensional Research | March 2016

The current level of security framework adoption is not the end of the story. There are many organizations that are planning to adopt additional frameworks in the coming year with CSF heading the list (14%), followed by CIS (12%) and ISO (9%). “Other” security frameworks to be adopted include SOC, Hitrust, and Cc2m2.



While PCI is currently slightly more common than the other frameworks, if we consider the current adoption of each security framework combined with the plans for adoption in the coming year, this small lead decreases. By the end of 2016, it should be expected that CSF (43%), CIS (44%), and ISO (44%) will all have equivalent levels of adoption, drawing closer to that of PCI (55%).



TRENDS IN SECURITY FRAMEWORK ADOPTION

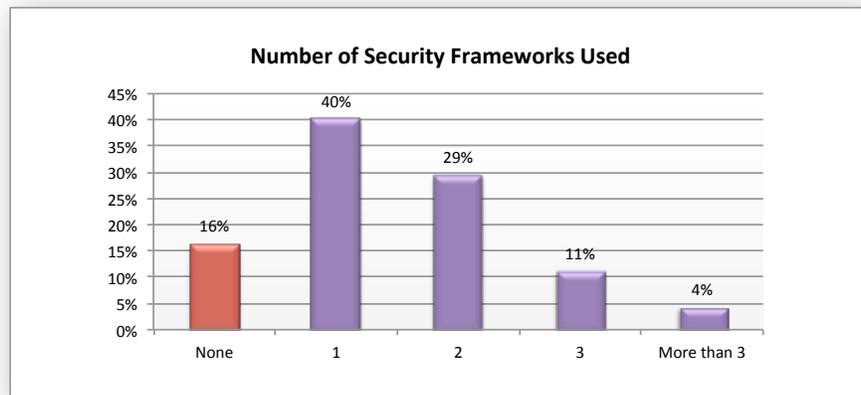
A SURVEY OF IT AND SECURITY PROFESSIONALS



Dimensional Research | March 2016

Use of multiple security frameworks common

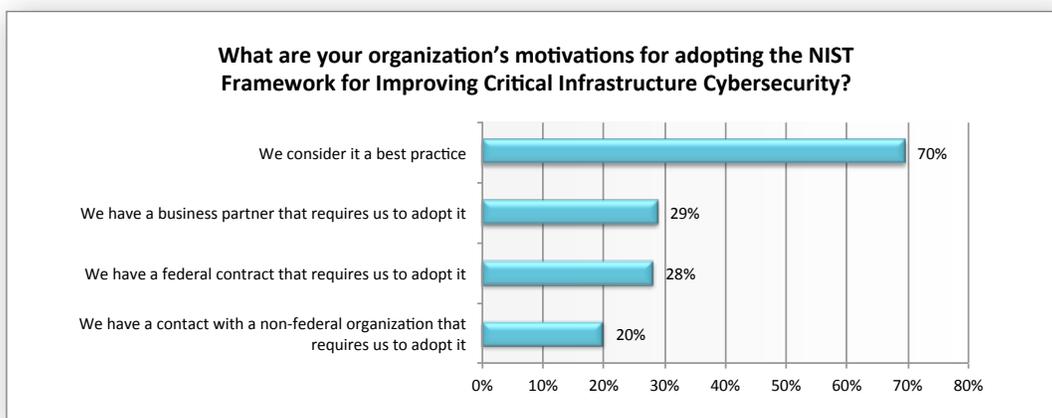
Security teams are searching for guidance, and in many cases they are getting it from multiple places. Close to half of organizations (44%) report that they are using multiple frameworks in their security program, including 15% that are using three or more. Only 40% use a single security framework.



Business partners and best practice both driving adoption

Security frameworks are frequently discussed in terms of compliance and regulations. The focus is on the security efforts that companies are required to make because of a business relationship, government, or certification mandate. While this does happen, this is not always the case. Many organizations are looking to security frameworks for guidance, even if they are not strictly required to follow them.

When we asked about motivations for adopting CSF, the security framework driven by the US government, the leading reason for adoption was simply that it was a best practice (70%). This was the most common reason for adopting CSF, far ahead of any requirement by a business partner (29%), federal contract (28%), or other organization (20%).



TRENDS IN SECURITY FRAMEWORK ADOPTION

A SURVEY OF IT AND SECURITY PROFESSIONALS

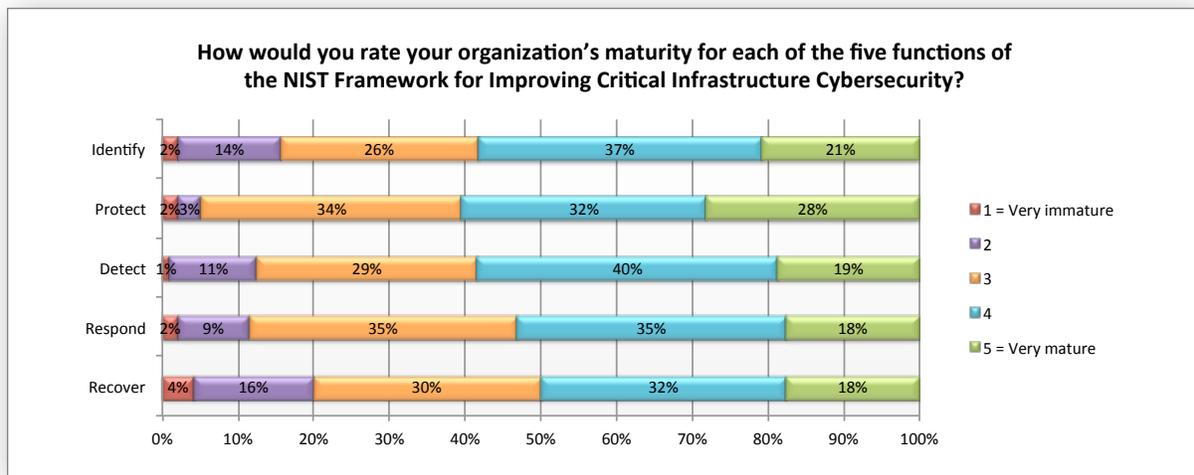


Dimensional Research | March 2016

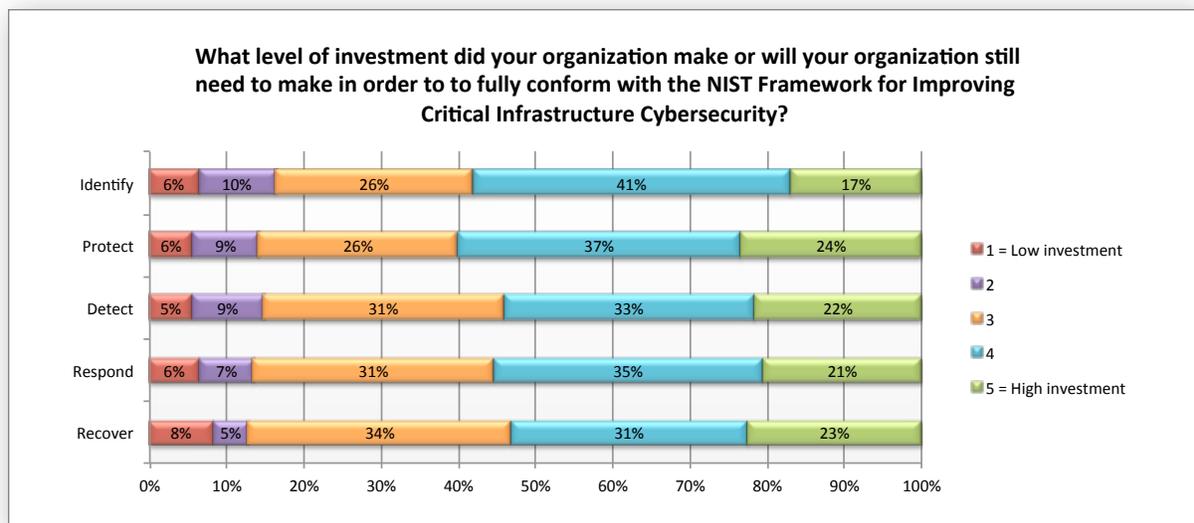
Adoption is a journey

It is important to point out that adoption of a security framework does not happen overnight. These security frameworks shape an organizations' security program over time and may take years to reach maturity.

We asked participants who reported adoption of CSF to rate their maturity along the five functions of the framework: Identify, Protect, Detect, Respond and Recover. The data shows there is little mastery of this framework. For most of the five functions (Identify, Detect, Respond Recover) only about 1 in 5 (from 18% to 21%) ranked their organization as very mature in their adoption. Protect was the most mature of the five functions across the organizations that use them with more than 1 in 4 (28%) saying they were very mature.



Mastery in the functions of CSF will require investment. More than half of those who have adopted CSF report that the investment needed to fully conform with each of the five functions will be high, indicating a 4 or 5 on a scale of 1-5 with 5 being the highest investment.



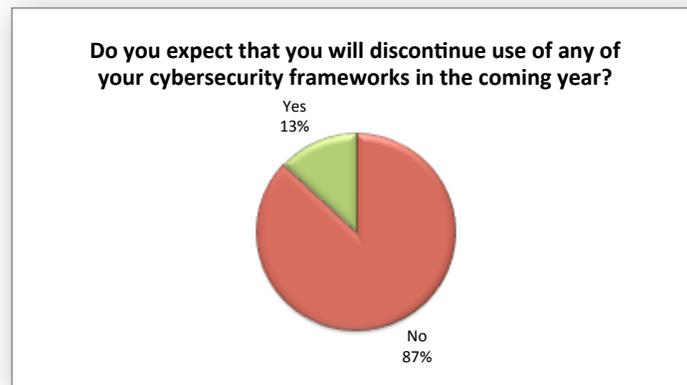
TRENDS IN SECURITY FRAMEWORK ADOPTION

A SURVEY OF IT AND SECURITY PROFESSIONALS



Dimensional Research | March 2016

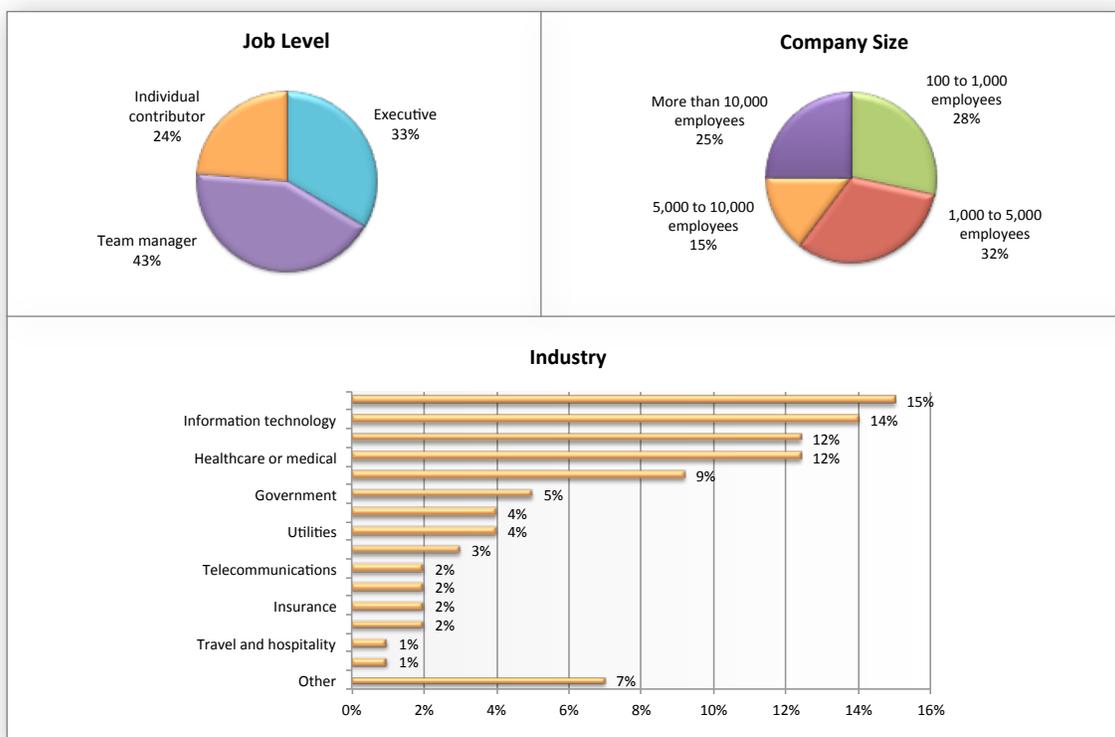
Interestingly, once a company has adopted a security framework, they very rarely discontinue use. When asked if they would be discontinuing use of any of their existing frameworks, only a few (13%) said that they would.



Survey Methodology and Participant Demographics

In February 2016, IT and security professionals in the United States 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 more.

A total of 338 qualified participants completed the survey. All participants were IT professionals with responsibility for security at companies with more than 100 employees. A wide range of job levels, company sizes, and vertical industries were represented.



TRENDS IN SECURITY FRAMEWORK ADOPTION

A SURVEY OF IT AND SECURITY PROFESSIONALS



Dimensional Research | March 2016

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.