CIS™ Center for Internet Security®

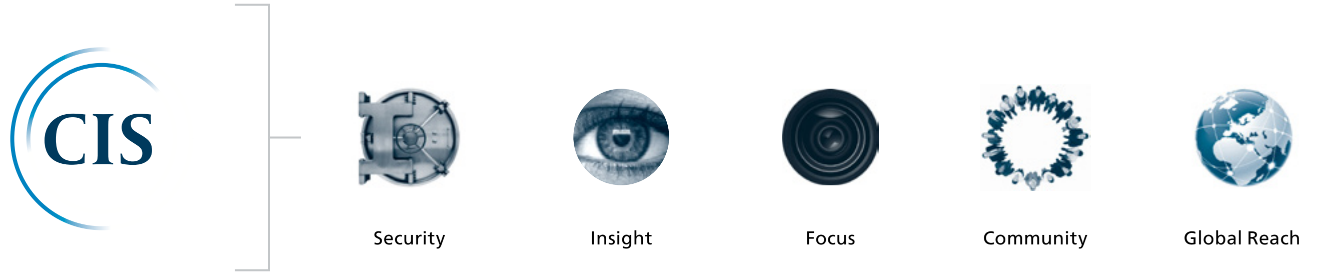
Confidence in the Connected World

2016 Year in Review

CIS harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

Our CIS Controls and CIS Benchmarks are born from the objective expertise of the cyber community to deliver confidence in the connected world. These recognized security best practices, together with our timely cyber intelligence resources, help organizations to start and stay secure.

Contents



Our New Identity

For the new CIS brand mark, capital serif letters were chosen to emphasize strength and trustworthiness, two attributes that speak to the proud history and solid reputation of the CIS organization, people, and products/services. The shape and form of the blue gradient circles are visual cues inspired by similar shapes that evoke CIS' brand attributes.

Welcome Message

John M. Gilligan
Chairman of the Board
and Interim Chief
Executive Officer

Steven J. Spano
Brig. Gen., USAF (Ret.)
President and
Chief Operating Officer

CIS continues to experience growth and expanded recognition as a global leader in cybersecurity for public and private sector organizations. As the global cyber threat evolves, the men and women at CIS have adapted the products and services that we provide to support this rapidly changing environment.

In 2016, we significantly expanded the functionality of our existing CIS products and services. We also successfully launched new cyber offerings to address emerging technologies such as cloud computing, and we continued the growth of our Multi-State Information Sharing & Analysis Center (MS-ISAC®) support capabilities.

CIS achieved several major milestones in 2016. The MS-ISAC passed the 1,000-member mark. In addition, 50 of the 56 states and territories eligible for monitoring under the Department of Homeland Security (DHS) Cooperative Agreement have implemented MS-ISAC's monitoring services. The CIS Benchmark Memberships also exceeded the 1,000-member milestone, with more than one-third coming from international public and private entities. Finally, the CIS Controls exceeded 43,000 downloads in 2016, and the Controls continue to gain traction as the go-to security framework when organizations seek technical guidance for implementing improved security.

As we look forward to 2017 and beyond, the CIS team continues to stay on the leading edge of cybersecurity solutions by pursuing innovative solutions and working collaboratively with communities and partners. Our goal continues to be achieving impact. We measure our progress by monitoring the ability of our global public and private sector partners and communities to defend against cyber threats.

CIS is committed to delivering confidence in the connected world because we believe everyone deserves a secure online experience.

Sincerely,

John M. Gilligan
Chairman of the Board
and Interim Chief Executive Officer

Steven J. Spano
Brig. Gen., USAF (Ret.)
President and Chief Operating Officer

Who We Are

CIS is a forward-thinking nonprofit entity that harnesses the power of the global IT community to safeguard private and public organizations against cyber threats.

Our CIS Controls and CIS Benchmarks are global standards and recognized best practices for securing IT systems and data against the most pervasive attacks.

These proven guidelines are continually refined and verified by a volunteer global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing & Analysis Center (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for state, local, tribal, and territorial governments.

$11 Million Cost Savings Achieved for the Public Sector Through Aggregate Cybersecurity Buys

1,039 CIS Benchmarks Global Members

140+ Secure Configuration Benchmarks

56 MS-ISAC memberships cover all 50 states, 5 territories, and Washington, D.C.

300+ Archived Secure Configuration Benchmarks

48 States Participated in MS-ISAC's 2016 Nationwide Cyber Security Review

470,455 Free Downloads of Active CIS Benchmarks (PDF format)

6.5 Trillion Records Analyzed Through the MS-ISAC Security Operations Center

43,032 Downloads of the CIS Controls

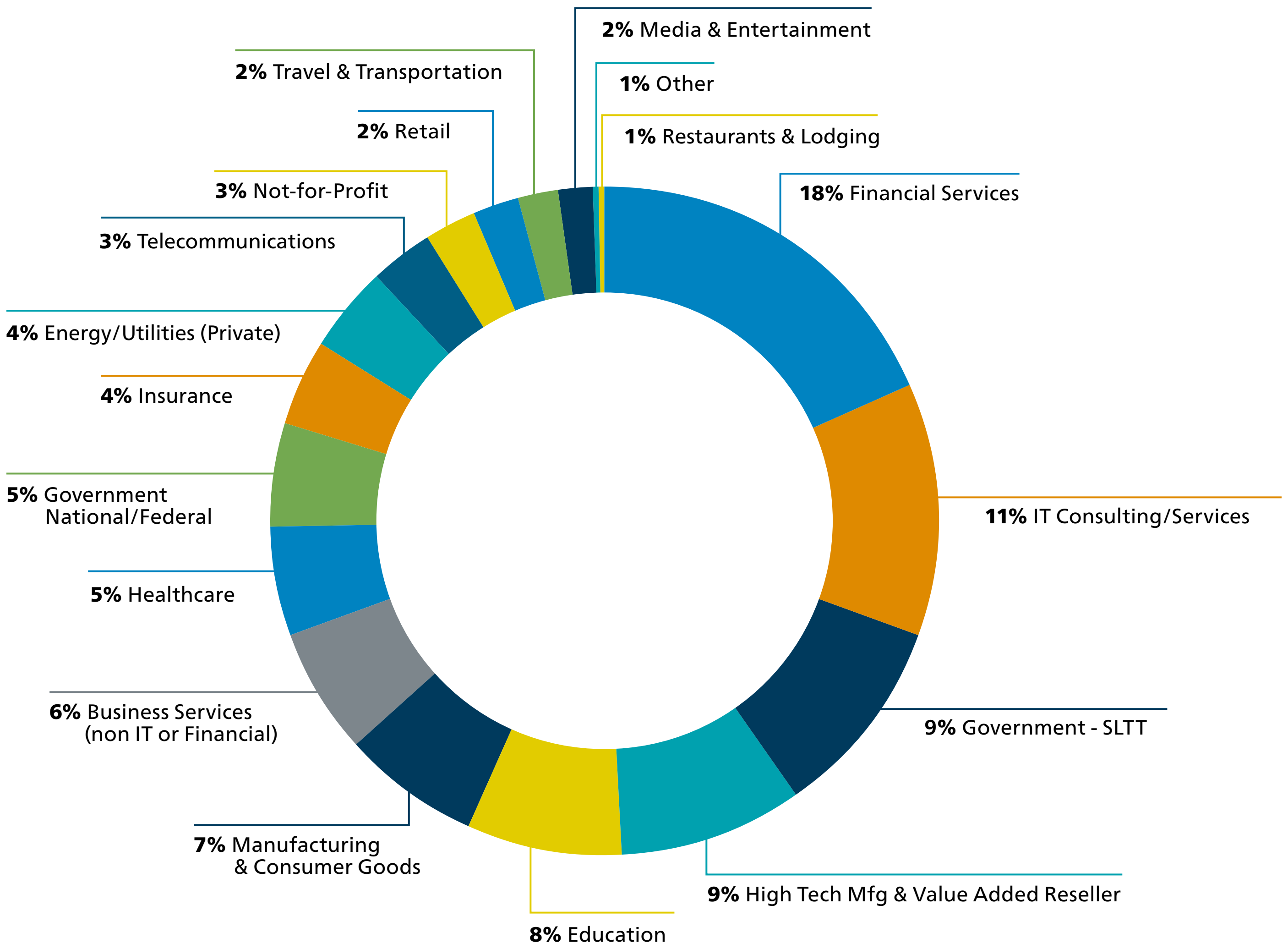
Issued Proclamations or Letters in Support of Recognizing National Cyber Security Awareness Month

48 states
2 territories
4 tribal nations
6 local governments

CIS Benchmarks

Reducing Risk Through Collaboration and Consensus
CIS has earned a global reputation for providing consensus-based industry best practice guidance that helps organizations assess and improve their cybersecurity. CIS Benchmarks resources include secure configuration benchmarks, automated configuration assessment tools and content, security metrics, and security software product certifications.

2016 CIS Benchmarks Members by Industry



CIS Benchmarks Membership

CIS Benchmarks membership includes organizations and users from virtually every industry sector, and ranges in size from independent consultants to Fortune 500 companies. Overall membership grew by more than 40 percent during 2016 to 1,039 enterprise members representing businesses, governments, universities, and other organizations from across the United States and around the globe.

More than 30 percent of the membership growth is in the international arena, reflecting the growing global recognition of the importance of consensus-based industry best practices available through CIS Benchmarks membership. CIS offers multiple membership categories, including discounted options for state, local, tribal, and territorial (SLTT) governments, academic institutions, and 501(c)(3) nonprofits.

CIS knows that a single breach can devastate an organization's reputation and kill customer confidence in their brand. That's why CIS augments our system-hardening guidelines with implementation and assessment tools to quickly secure known vulnerabilities. CIS provides expert intelligence and incident response resources to protect organizations against evolving threats. These efforts ensure that as our CIS community grows, we'll leave nothing to chance in the battle for online security.

CIS Benchmarks Development

- 64 Benchmarks were developed in 2016, along with 152 derivatives that include machine consumable content.
- 146 of the latest versions of the Benchmarks are publicly available.
- 327 archived Benchmarks versions are still available for download.

Hardened Images Development

During 2016, CIS expanded our Amazon Web Services (AWS) hardened machine images (AMIs) offerings into Marketplace, GovCloud, and the Intelligence Community (IC) regions.

CIS now has 19 AMIs available in the AWS Commercial Marketplace, 17 in the GovCloud region, and 19 in the IC region. We continue to develop a strong partnership with Amazon Web Services by participating in several conferences to promote security in the cloud using our hardened images and our AWS Foundations Benchmarks.

A Pioneer in Cyber Protection: CIS was instrumental in establishing the first guidelines for systems hardening at a time when there was little online security leadership. As a forward-thinking nonprofit organization, we pioneered the formation of a volunteer IT community to continuously validate our work.

CIS SecureSuite™

In late 2016, CIS announced the addition of several new features that significantly enhance the functionality of our signature product suite. The updated and enhanced CIS tools include the CIS Benchmarks annotated with CIS Controls, multi-component CIS-CAT Pro, and CIS WorkBench—all of which are now available through a CIS SecureSuite Membership. The CIS SecureSuite Membership provides access to a wide range of tools and resources to help public and private entities improve their cybersecurity posture.

This landmark update offers users a unique combination of the powerful CIS Benchmarks standards with the globally recognized guidance of the CIS Controls best practices. By linking these two proven cybersecurity resources in a suite of integrated tools, users have unprecedented insight and guidance on how to protect their critical systems against cyber attacks.

We were proud to announce the general availability of our new Benchmark Community Platform, known as "CIS WorkBench," in 2016. The new platform provides unprecedented functionality to our members including:

- Benchmark customization features that give members the ability to easily tailor recommendations within a Benchmark from our migrated communities.
- Ability to easily export the Benchmarks tailored in Adobe® PDF, Microsoft® Word, and Microsoft® Excel formats.
- New capability to export Benchmarks in XML and OVAL formats.

WorkBench also automates the workflow for our communities to develop and track changes and versions with powerful new features. CIS has successfully migrated more than 65 communities to the new platform. This new tool is a cornerstone of CIS SecureSuite.

A second component of CIS SecureSuite developed in 2016 is our Controls Annotated Benchmarks. With integration of our secure configuration standards and CIS Controls, our members benefit by having two separate views of assessments provided by CIS-CAT, a configuration assessment/audit software tool available to CIS Benchmarks members. The first view is the usual assessment scoring based on Benchmarks configuration standards; the second view is an assessment shown as a Controls view from a mapping from Controls to Benchmarks and based on the same Benchmark configuration standards.

These updates allow CIS to grow our coverage and meet the demands of our member base. While these updates will help provide a foundation for cybersecurity, they're just a harbinger of many things CIS will offer our members in the future.

OVAL 5.11.2 Release

CIS released version 5.11.2 of the OVAL Language, working in cooperation with the OVAL Community. This substantial achievement improves the coverage and efficacy of the OVAL Language by incorporating Mac OS and Cisco schemas to the language, and addresses more than 60 recorded issues.

OVAL is an important component of the security automation ecosystem. The language provides a means to describe assessment checks for endpoint vulnerability, configuration, and inventory tasks commonly found in enterprise IT operations, especially those that follow a prescribed set of best practices, such as those found in the CIS Controls. The repository provides a publicly and freely available source of vulnerability checks expressed using the OVAL Language.

CIS is immensely grateful for all those in the IT community who contributed to reviewing and testing the 5.11.2 OVAL Language release. Their hard work and dedication are crucial to the OVAL Language's success.

CIS Controls

Overview

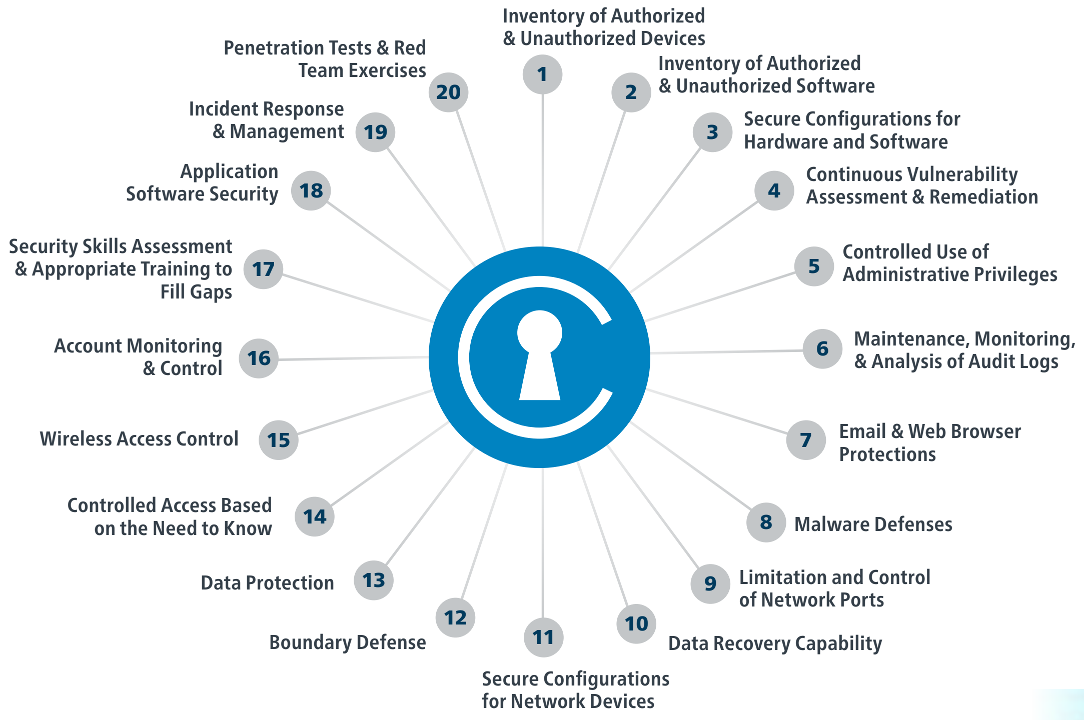
The CIS Controls program continued to grow and mature its efforts to increase universal awareness and adoption in 2016.

At the close of 2015, the newly released Version 6.0 had been downloaded more than 10,000 times. By end of 2016, the **CIS Controls had been downloaded 43,032 times,** an average rate of over 3,500 downloads per month.

During 2016, a significant focus for the CIS Controls program was outreach to organizations that had already implemented, or were in the process of implementing, the Controls. It proved to be an invaluable opportunity to gather and analyze feedback from Controls users. Surveys, case studies, and interviews broadened our understanding of CIS Controls implementations. This led to improvements in the existing CIS Controls content as well as the development of additional content targeted to specific user needs. One such effort was the development of Version 6.1 of the CIS Controls, which reintroduced a prioritization scheme to help organizations identify which Controls are "foundational" and which are "advanced."

> *The security industry is crowded with vendors selling unique solutions based on their own product or services vision. The strength of CIS lies in objectivity. Our CIS Benchmarks and CIS Controls are curated by experienced IT practitioners focused on performance, not profits. This consensus process ensures CIS remains the objective, referenced cybersecurity standard in industry, government, and academia.*

CIS Controls


1 Inventory of Authorized & Unauthorized Devices
2 Inventory of Authorized & Unauthorized Software
3 Secure Configurations for Hardware and Software
4 Continuous Vulnerability Assessment & Remediation
5 Controlled Use of Administrative Privileges
6 Maintenance, Monitoring, & Analysis of Audit Logs
7 Email & Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports
10 Data Recovery Capability
11 Secure Configurations for Network Devices
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring & Control
17 Security Skills Assessment & Appropriate Training to Fill Gaps
18 Application Software Security
19 Incident Response & Management
20 Penetration Tests & Red Team Exercises

2016 Program Accomplishments

The CIS program team made great strides in Content Development, Awareness and Adoption, and Customer Engagement.

Content Development and Enhancement Activities

- In 2016, the CIS Critical Security Controls were updated from V.6.0 to V.6.1 to reintroduce prioritization categories among the sub-controls.
- The Controls team published the following guides:
  - *An Executive Summary of the CIS Controls*
  - *Practical Guidance for Implementing the Controls*
  - *CIS Controls Privacy Implications*
  - *The CIS Community Attack Model* white paper

Awareness and Adoption Promotion Activities

- Documented 28 case studies of user experience with the CIS Controls.
- Presented 25 keynote presentations at various security events.
- Participated in more than 40 media interviews including *Healthcare IT News* and *SC Magazine.*

"The set of 20 Controls constitutes a minimum level of security—a floor—that any organization that collects or maintains personal information should meet."

Kamala D. Harris
California Attorney General
February 2016

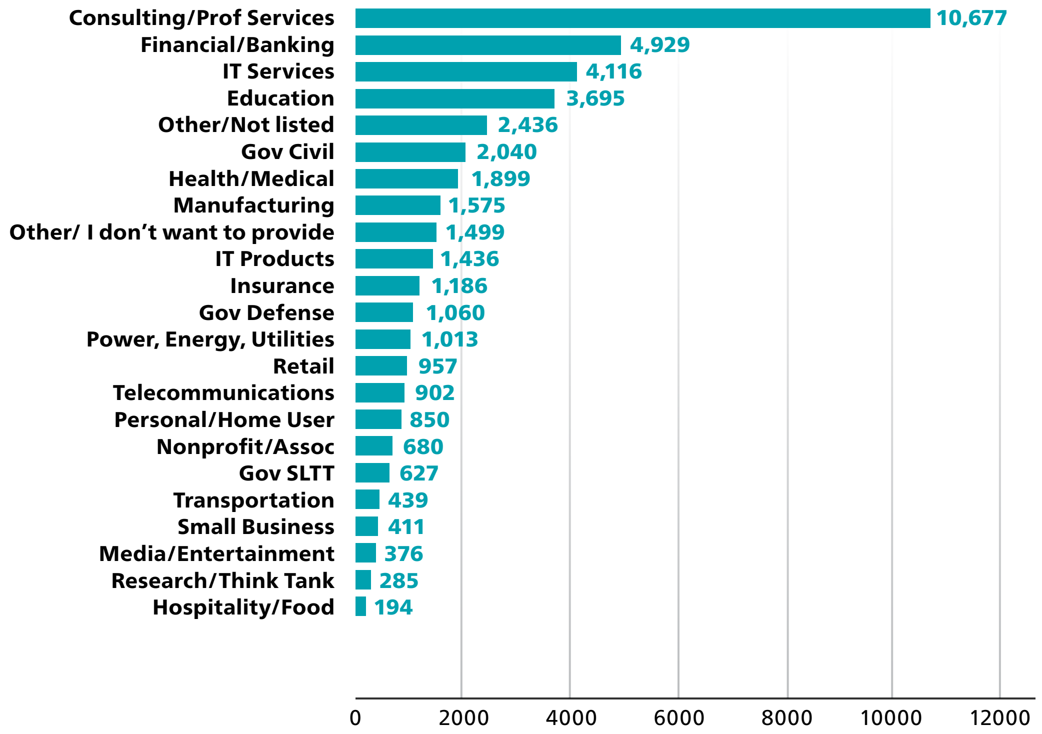
In addition, the CIS Controls were referenced by the following organizations:

- The European Telecommunications Standards Institute (ETSI) adopted and published the CIS Controls and several companion guides.
- In its 2016 California Data Breach Report, the Office of the California Attorney General recommended the CIS Controls, stating they are the "minimum level of information security that all organizations that collect or maintain personal information should meet."
- The National Highway Traffic Safety Administration recommended the CIS Controls in its draft security guidance to automotive manufacturers.
- The National Institute of Standards and Technology (NIST) again included a mapping of the CIS Controls in Version 1.1 of the Cybersecurity Framework.

Customer Engagement and Support Activities
The Controls team began a campaign of regular outreach to users to capture feedback about their experiences:

- Conducted a survey of organizations that have implemented the CIS Controls.
- Collaborated with the Tenable® network security company on a *Cybersecurity Frameworks and Foundational Security Controls* survey.

2016 CIS Controls Downloads By Industry



There is a constant onslaught of destructive forces threatening the integrity of most critical systems and data. CIS empowers organizations to be vigilant in defending the connected technologies that drive business success. Our CIS Controls and CIS Benchmarks set a secure foundation for the world's most progressive public and private entities. They are endorsed by leading IT security vendors and governing bodies. More than guidelines, these are global industry best practices that will move organizations from compliance to confidence online.

MS-ISAC

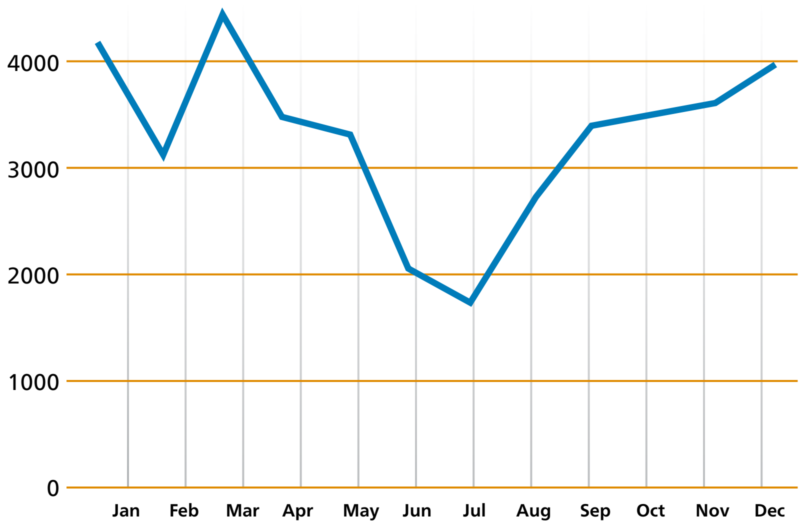
The Multi-State Information Sharing & Analysis Center (MS-ISAC) is the U.S. Department of Homeland Security's (DHS) recognized resource for collaborative cyber information sharing and analysis among state, local, tribal, and territorial (SLTT) governments and fusion centers.

Operations is the technical core of the MS-ISAC, providing centralized analytical and subject matter expertise, while maintaining the most comprehensive national situational awareness of the risks to, and cybersecurity protections undertaken by, SLTT governments. MS-ISAC Operations has several functional areas, which are highlighted below.

- **Security Operations Center (SOC)** provides 24/7 monitoring of cybersecurity threats and attacks that could impact SLTT governments.
- **Computer Emergency Response Team (CERT)** provides SLTT governments with malware analysis, computer and network forensics, malicious code analysis mitigation, and incident response.
- **Intel Analysis Team (Intel)** makes informed assessments about cyber trends, actors, and tactics, techniques, and procedures (TTPs) affecting SLTT governments.
- **National Liaison Team (NLT)** is assigned to the National Cybersecurity and Communications Integration Center (NCCIC), a 24/7 operations coordinating center for U.S. cybersecurity efforts established by DHS.
- **Vulnerability Management Program (VMP)** provides SLTT governments with vulnerability assessments, phishing engagements, penetration testing, and Web profiling.

The MS-ISAC SOC analyzed more than 6.5 trillion records in 2016 from its network monitoring service. Events generated affecting SLTT governments varied widely throughout 2016, peaking at more than 4,489 events in March and declining to a low of 1,776 events in July. The MS-ISAC attributed these variations to a range of factors impacting the cyber threat landscape, including malware changes, dissemination vectors, arrests/takedowns, etc.

2016 MS-ISAC Event Notifications

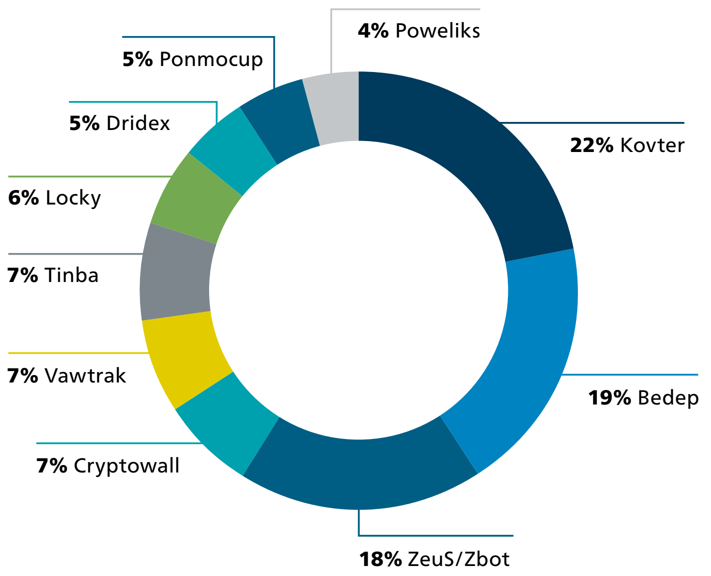


The SOC sent almost 40,000 notifications regarding malware and malicious activity and more than 34,000 notifications regarding compromised credentials, infected hosts, vulnerable websites, and defaced websites in 2016. The SOC also sent out 192 Cybersecurity Advisories.

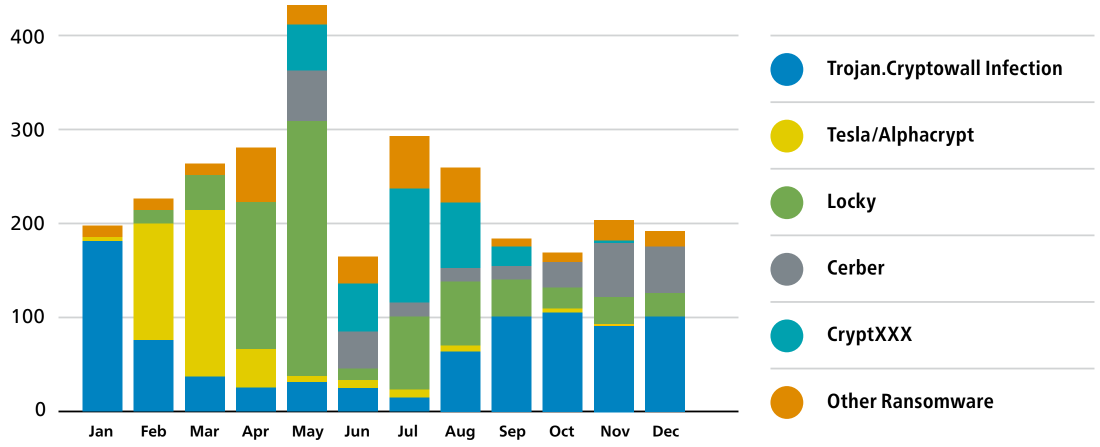
The CERT handled 171 incidents in 2016, and the majority of incidents focused on ransomware, compromised servers, and malware infections.

Malware in 2016
Efforts by the Intel Team resulted in the production of 87 cyber threat intelligence products throughout the year, and an additional 56 Intelligence Information Reports distributed to the U.S. Intelligence Community. The team also responded to more than 200 cyber threat actor incidents.

Malware



Ransomware



Vulnerability Management Program (VMP) staff profiled an average of 30,000 domains each month, to check for out-of-date software and notify domain owners when identified. In addition, the VMP team regularly performed penetration tests, phishing engagements, and vulnerability assessments.

The Ransomware 101 Roadshow

FINANCIAL SERVICES ISAC
paloalto NETWORKS
DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION
UNITED STATES SECRET SERVICE
Symantec.
MS-ISAC
Multi-State Information Sharing & Analysis Center
NH-ISAC
NATIONAL HEALTH · ISAC

Ransomware
In the fall of 2016, the Multi-State ISAC partnered with the National Health Information Sharing & Analysis Center (NH-ISAC), Financial Sector Information Sharing & Analysis Center (FS-ISAC®), Federal Bureau of Investigation (FBI), and U.S. Secret Service (USSS) to host 15 events across the nation that were sponsored by Symantec® and Palo Alto Networks®.

> *IT professionals often feel isolated as they are constantly expected to keep systems running securely, fix problems immediately, and otherwise keep to themselves. CIS connects these professionals to a worldwide community fueled by trust and collaboration.*

Bringing SLTT Government Professionals Together
The MS-ISAC has fostered a trusted environment between and among its SLTT government partners and with DHS. MS-ISAC conducts monthly membership webinar meetings that provide an interactive forum for sharing information on cybersecurity issues important to the SLTT government cyber domain. DHS participates in these webcasts, providing the opportunity for them to connect with SLTT government officials on a monthly basis.

The MS-ISAC Executive Committee consists of representatives who are elected by the MS-ISAC members to assist in providing strategic guidance and recommendations for the MS-ISAC. The members also participate in a number of issue-specific working groups to target the areas of most concern to the members.

Membership in the MS-ISAC grew by 43 percent in 2016 to a total of 1,288, representing all 50 states, 1,123 local governments, six U.S. territories, and 31 tribal nations.

The MS-ISAC works closely with other prominent organizations to continue to build trusted relationships to further enhance the cybersecurity posture of the nation. Outreach and collaboration includes working with the National Governors Association (NGA), Governors Homeland Security Advisors Council (GHSAC), National Association of State Chief Information Officers (NASCIO), National Association of Counties (NACo), National Cyber Security Alliance (NCSA), and many others. CIS also partners with the other national critical infrastructure sector Information Sharing & Analysis Centers (ISACs) through the National Council of ISACs.

The Annual Meeting is the cornerstone MS-ISAC event each year. The meeting focuses on working sessions to address specific MS-ISAC objectives, with the ultimate goal of working collectively to enhance our overall cybersecurity posture.

The 2016 Annual Meeting was the largest-attended to date, with 389 attendees representing all 50 states, four territories, eight tribal nations, 102 local governments, and 51 fusion centers.

2016 MS-ISAC Annual Meeting attendees

Education and Awareness

An important part of the CIS mission is to raise awareness and provide resources that help users stay informed about the ever-changing cyber threat landscape. MS-ISAC helps achieve this mission in a number of ways, including the development and distribution of monthly cyber-tip newsletters (which organizations can brand with their own logos), bimonthly educational webcasts (with registrants in 2016 from all 50 states, 25 tribes, several U.S. territories, and 17 countries), a daily cyber-tip feed on the CIS public website, and a variety of guides, white papers, and other resources.

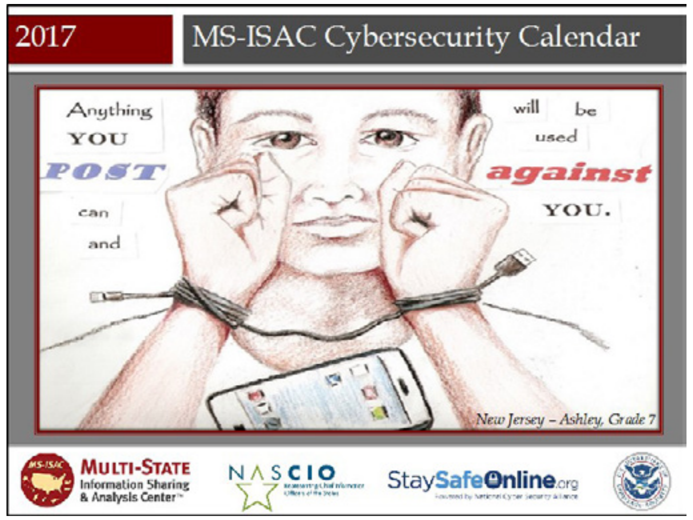
National Cyber Security Awareness Month (NCSAM)

MS-ISAC also coordinates a proclamation campaign, inviting each state governor and local elected official to sign a proclamation in support of NCSAM, thus showing the importance of cybersecurity at leadership levels. In 2016, 48 state governors issued proclamations or letters of support, along with two U.S. territories, four tribal nations, and six local government officials.

National *Kids Safe Online Poster Contest*

One of MS-ISAC's most popular awareness activities is the annual *Kids Safe Online Poster Contest,* which encourages young people to use the Internet safely and securely. The contest engages young people as they create messages and images to communicate to their peers the importance of staying safe online. Then, 13 entries are selected and appear in the national calendar distributed each year as part of the Awareness Month toolkit. The national winner's artwork is selected for the special honor of the cover of the calendar. In 2016, MS-ISAC received more than 200 poster entries from 13 states for the *Kids Safe Online Poster Contest.*

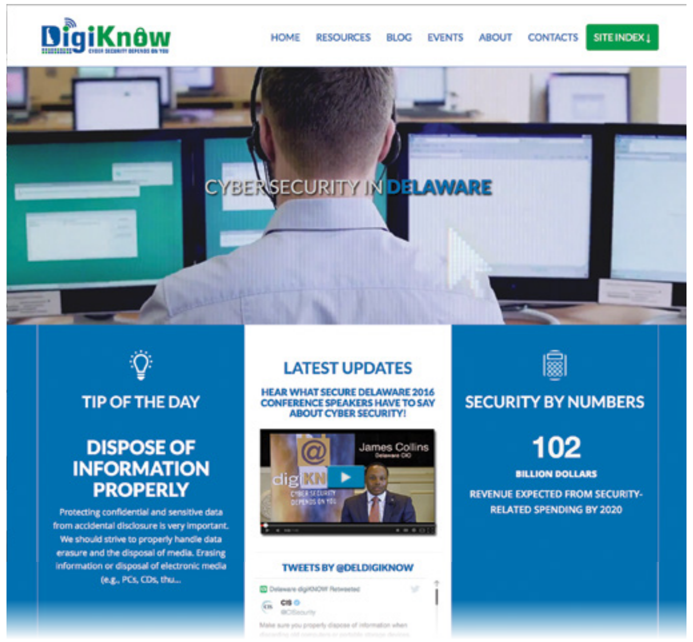
The 2017 MS-ISAC Cybersecurity Calendar


2017
MS-ISAC Cybersecurity Calendar
Anything
YOU
POST
can
and
will be
used
against
YOU.
New Jersey – Ashley, Grade 7
MULTI-STATE Information Sharing & Analysis Center
NASCIO
StaySafeOnline.org

National *Best of the Web Contest*

MS-ISAC launched its eighth annual *Best of the Web Contest* in August. The MS-ISAC's Education and Awareness Workgroup judged cybersecurity websites from all 50 state governments and a number of local and territorial governments. MS-ISAC announced the winning entries during its November monthly membership meeting.

2016 Winners of MS-ISAC's *Best of the Web Contest*



DigiKnow — CYBER SECURITY DEPENDS ON YOU

HOME RESOURCES BLOG EVENTS ABOUT CONTACTS SITE INDEX ↓

CYBERSECURITY IN DELAWARE

TIP OF THE DAY

DISPOSE OF INFORMATION PROPERLY

Protecting confidential and sensitive data from accidental disclosure is very important. We should strive to properly handle data erasure and the disposal of media. Erasing information or disposal of electronic media (e.g., PCs, CDs, thu...

LATEST UPDATES

HEAR WHAT SECURE DELAWARE 2016 CONFERENCE SPEAKERS HAVE TO SAY ABOUT CYBER SECURITY!

James Collins, Delaware CIO

TWEETS BY @DELDIGIKNOW

Delaware digiKNOW Retweeted

CIS @CISecurity

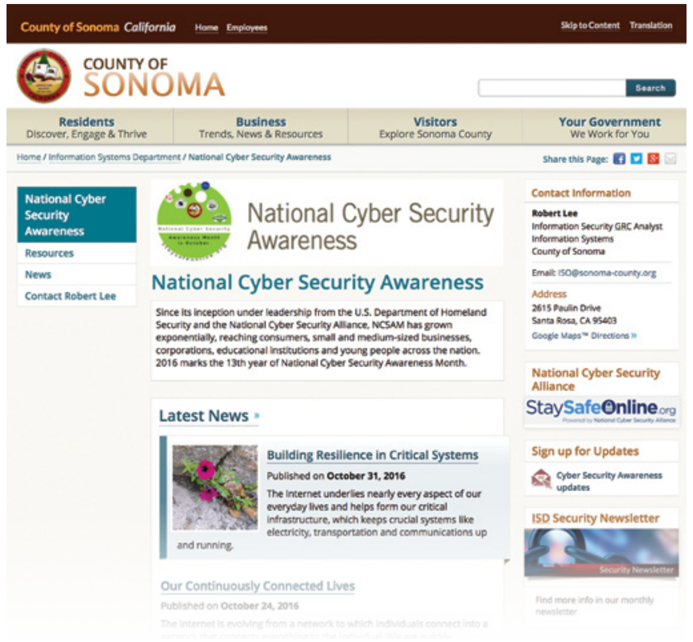
Make sure you properly dispose of information when

SECURITY BY NUMBERS

102 BILLION DOLLARS

REVENUE EXPECTED FROM SECURITY-RELATED SPENDING BY 2020

State Government
Delaware



County of Sonoma California Home Employees Skip to Content Translation

COUNTY OF SONOMA

Search

Residents — Discover, Engage & Thrive | Business — Trends, News & Resources | Visitors — Explore Sonoma County | Your Government — We Work for You

Home / Information Systems Department / National Cyber Security Awareness

Share this Page:

National Cyber Security Awareness
Resources
News
Contact Robert Lee

National Cyber Security Awareness

National Cyber Security Awareness

Since its inception under leadership from the U.S. Department of Homeland Security and the National Cyber Security Alliance, NCSAM has grown exponentially, reaching consumers, small and medium-sized businesses, corporations, educational institutions and young people across the nation. 2016 marks the 13th year of National Cyber Security Awareness Month.

Latest News »

Building Resilience in Critical Systems
Published on **October 31, 2016**
The Internet underlies nearly every aspect of our everyday lives and helps form our critical infrastructure, which keeps crucial systems like electricity, transportation and communications up and running.

Our Continuously Connected Lives
Published on October 24, 2016
The Internet is evolving from a network to which individuals connect into a network that connects everything to the individual. We are quickly

Contact Information
Robert Lee
Information Security GRC Analyst
Information Systems
County of Sonoma
Email: ISO@sonoma-county.org

Address
2615 Paulin Drive
Santa Rosa, CA 95403
Google Maps™ Directions »

National Cyber Security Alliance
StaySafeOnline.org

Sign up for Updates
Cyber Security Awareness updates

ISD Security Newsletter
Security Newsletter
Find more info in our monthly newsletter

Local Government
Sonoma County, California

The Nationwide Cyber Security Review (NCSR) is an annual voluntary self-assessment survey designed to evaluate cybersecurity management programs within SLTT governments. The core of the NCSR is the Control Maturity Model, which is used to measure how effective an organization's security program is at deploying a given control, in light of identified risks to that organization's operations.

DHS partnered with CIS, along with the National Association of State Chief Information Officers and the National Association of Counties, to develop and conduct the Review, which took place for the fifth time in 2016.

CIS substantially updated the NCSR in 2015 to link the questionnaire content and responses to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. This was done both to promote the efforts of NIST in creating a holistic risk-based cybersecurity framework and to provide an assessment organizations can use to better understand how their cybersecurity efforts align with the framework and associated best practices.

Participation in the 2016 NCSR included representatives from 48 states, 122 local governments, 285 state agencies, and nine tribal nations, representing the largest NCSR to date. Organizations that participated not only received access to their own results, but also were able to anonymously compare how they scored in comparison with their peers. This allowed each organization to establish their own baseline and also helped identify priority areas by understanding gaps in their cybersecurity programs.

The 2016 NCSR represents a first step for the SLTT community to collaboratively adopt the principles of the Framework. By developing a baseline of cybersecurity maturity using the NCSR, the MS-ISAC partner community comes together and identifies which areas should be prioritized as the cybersecurity risk landscape continues to evolve. One such area that will need collaboration to address is the disparity in capabilities between state and local governments.

CIS CyberMarket

The procurement process for state and local governments can be time-consuming, costly, and complex. For many entities, a lack of staff and technical expertise, coupled with budget constraints, can hinder their ability to successfully implement the security controls needed to defend against ever-increasing cybersecurity threats.

In 2016, CIS CyberMarket, formerly called the CIS Trusted Purchasing Alliance, entered its fifth year. This program leverages the collective purchasing power of the public sector to collaborate with leading cybersecurity providers. CIS CyberMarket allows all participants the ability to improve their cybersecurity posture at a substantially lower cost than they could achieve individually.

Product and service choices for the program's aggregate buys are driven by the unique needs of state and local governments and the ability of potential vendors to positively impact and improve their cybersecurity infrastructure. CIS CyberMarket oversees a review board of government partners who carefully review and select potential offerings, and then works with our rigorously vetted industry partners to negotiate volume discount purchasing opportunities.

During 2016, 420 state, local, tribal, and territorial government organizations, not-for-profits, and public healthcare and educational institutions took advantage of aggregate purchasing opportunities, an increase of nearly 32 percent from 2015. In total, participants saved more than $11 million in procurement costs in 2016 through CIS CyberMarket.

CIS Leadership

Officers & Board of Directors

Officers

John M. Gilligan
Chairman and Interim Chief Executive Officer
President and Chief Operating Officer
Schafer Corporation

Karen S. Evans
Treasurer
Partner
KE&T Partners, LLC

Deirdre O'Callaghan
Secretary and Chief Counsel
CIS

Steven J. Spano
Brig. Gen., USAF (Ret.)
President and Chief Operating Officer
CIS

Directors

Jack Arthur
Executive Vice President
Octo Consulting Group

Michael Assante
ICS Director
SANS Institute

Dr. Ramon Barquin
President and Chief Executive Officer
Barquin International

Jane Holl Lute

Bruce Moulton
Vice President (Ret.)
National Grand Bank

Alan Paller
Founder and Director of Research
SANS Institute

Franklin Reeder
Co-Founder
CIS

Richard Schaeffer
Advisor
Riverbank Associates, LLC

Phil Venables
Managing Director and
Chief Information Risk Officer
Goldman Sachs

Executive Team

Kerry Coffey
Senior Vice President
Business Development

Thomas Duffy
Senior Vice President
Operations and Services
Chair, Multi-State ISAC

Richard J. Licht
Chief Administrative Officer

Kathleen Patentreger
Senior Vice President of Programs

Tony Sager
Senior Vice President and
Chief Evangelist

Albert Szesnat
Chief Financial Officer

CIS Center for Internet Security®

Organizations try to succeed and innovate every day
through adversity of persistent cyber attacks.

By sharing the collective knowledge and innovation
of our members, we continuously strengthen each other.

For more information about CIS
Contact: Barbara Ware
Director of Communications
Email: Barbara.Ware@cisecurity.org

31 Tech Valley Drive
East Greenbush, New York 12061
518.266.3460
Fax 518.266.2085
www.cisecurity.org

Follow Us on Twitter
twitter.com/CISecurity

Find Us on Facebook
facebook.com/CenterforIntSec

Join Us on LinkedIn
linkedin.com/company/122681

Watch Us on YouTube
youtube.com/user/TheCISecurity