



Center for Internet Security[®]

2015 ANNUAL REPORT





Contents

Welcome Message	4
2015 at a Glance	6
2015 Highlights	8
Security Benchmarks	8
CIS Critical Security Controls	12
Integrated Intelligence Center	15
Multi-State Information Sharing & Analysis Center	23
Making Security Affordable	27
CIS in the Spotlight	28
CIS Cares	28
Financials	29
CIS Leadership	30
Officers and Board of Directors	30
Executive Team	30
2015 Leadership Transitions	31

Welcome Message

Since its creation in 2000, the Center for Internet Security (CIS) has established itself as a valued and trusted resource for both the public and private sectors, and has grown its mission, staff, and programs to become an internationally recognized authority in cybersecurity.

Through programs like CIS Critical Security Controls™, CIS Security Benchmarks, and the Multi-State Information Sharing & Analysis Center (MS-ISAC™), CIS continues to be a driving force for improving cybersecurity by undertaking initiatives to help our partners detect, defend, and respond to threats.

MS-ISAC held its largest Annual Meeting to date in 2015, and across the board the members highlighted the vital importance of MS-ISAC in providing enhanced situational awareness and on-call support. Indeed, membership in MS-ISAC expanded in 2015 to include, among other new relationships, collaboration with fusion centers across the country. Local government participation in MS-ISAC now comprises nearly 48% of the U.S. population.

CIS Critical Security Controls Version 6.0 was released in 2015, along with measurable increases noted in their adoption and use. By the end of the year, the CIS Controls had been downloaded 13,844 times. Three new companion guides expanded the ecosystem of complementary tools to support wider uptake of the CIS Controls.

CIS has also grown our business lines. We now have more than 700 Security Benchmarks members with more than 30% of the membership growth in the global arena, reflecting the growing international recognition of the importance of our consensus-based industry best practices.

We are proud of our successes but also recognize that there is much more to be done. CIS will continually fine-tune our business processes and operations to be as efficient and effective as possible. As we move forward in 2016 and beyond, we will continue to strive for excellent service, innovative solutions, and collaborative approaches that further our mission of enhancing cybersecurity readiness and response.



John M. Gilligan
Chairman of the Board



Jane Holl Lute
Chief Executive Officer

Sincerely,

A handwritten signature in black ink, appearing to read "John M. Gilligan".

John M. Gilligan
Chairman of the Board

A handwritten signature in black ink, appearing to read "Jane Holl Lute".

Jane Holl Lute
Chief Executive Officer

Who We Are

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 & Analysis Center (MS-ISAC), CIS Security Benchmarks, and CIS Critical Security Controls.

Our Mission

Our mission is to identify, develop, validate, promote, and sustain best practices in cybersecurity. We're dedicated to delivering world-class security solutions to prevent and rapidly respond to cyber incidents. Ultimately, our goal is to build and lead communities to enable an environment of trust in cyberspace.



2015 at a Glance



\$8 Million

Cost Savings Achieved for the Public Sector
Through Aggregate Cybersecurity Buys

736

Security Benchmarks
Global Members



50

All 50 States Participated
in MS-ISAC's 2015 Nationwide
Cyber Security Review

48%

Local Government
MS-ISAC Members
Represent 48% of the
U.S. Population



100+

Secure Configuration Benchmarks
Across 14 Technology Groups

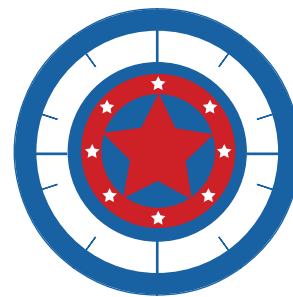


13,844

Downloads of the
CIS Critical Security Controls

78

Fusion Centers Participating
in the CIS Integrated
Intelligence Center



Recognition

48 States, 2 Territories, and 35 Local Governments
Issued Proclamations or Letters in Support of
Recognizing National Cyber Security Awareness Month

3 Trillion

Records Analyzed
Through the CIS Security
Operations Center



2015 Highlights



SECURITY BENCHMARKS

Reducing Risk Through Collaboration and Consensus

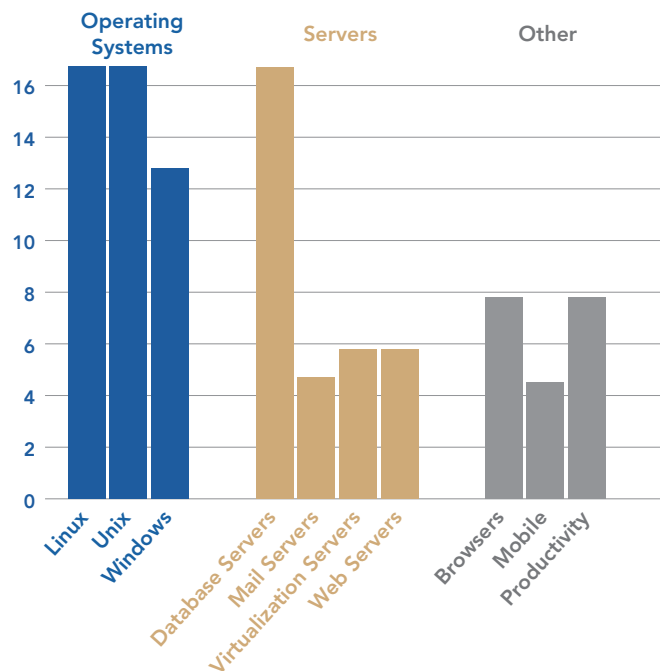
Since its creation in 2000, CIS has built a worldwide reputation for providing consensus-based industry best practice guidance that helps organizations to assess and improve their cybersecurity. These CIS Security Benchmarks resources include secure configuration benchmarks, automated configuration assessment tools and content, security metrics, and security software product certifications.

Secure Configuration Benchmarks

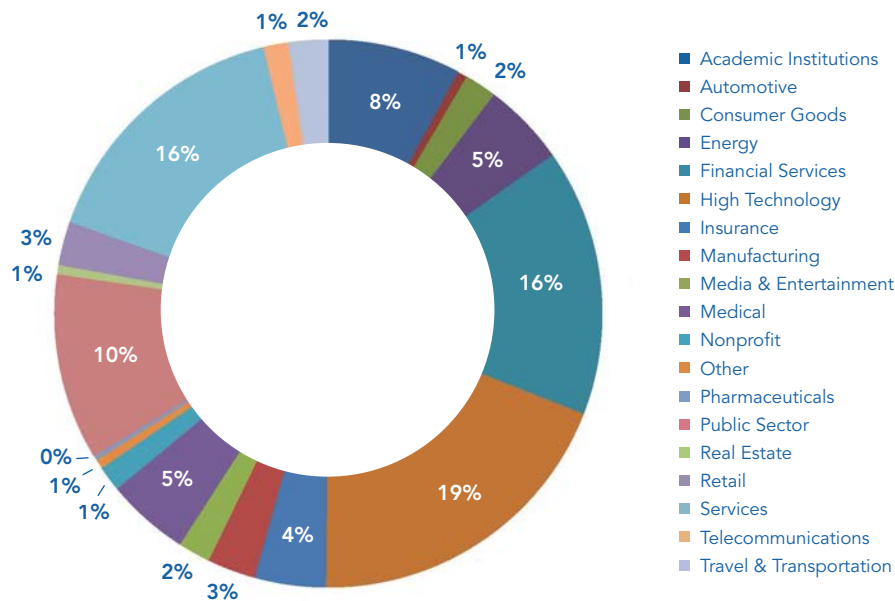
The CIS Benchmarks provide guidance on the security-focused configuration controls that should be applied for a wide range of technologies, specific procedures on how to implement those recommendations, and audit procedures to then verify that those controls are correctly implemented. The Benchmarks span the most commonly used IT systems and technology groups, including server and desktop operating systems, Web browsers, mobile devices, and more.

We released 56 new Benchmarks throughout the year and achieved a 201% increase in automation artifacts delivered in conjunction with some of our Benchmarks, releasing 84 automation artifacts.

2015 Benchmarks Produced by Category



Security Benchmark Members by Industry in 2015



CIS Security Benchmarks Membership

CIS Security 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 over 37% during 2015 to 736 enterprise members, representing businesses, governments, universities and more, from across the United States and around the globe. More than 30% 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 Security Benchmarks membership. CIS offers multiple membership categories, including discounted options for State, Local, Tribal, and Territorial (SLTT) governments.

Configuration Assessment Tool (CIS-CAT)

A cornerstone of CIS Security Benchmarks resources is CIS-CAT, our Configuration Assessment Tool. CIS-CAT is a powerful resource for analyzing and monitoring the security status of information systems and applications and the effectiveness of internal security processes. CIS-CAT enables the assessment of multiple systems simultaneously by integrating CIS-CAT with system management utilities, helping organizations to provide fast, detailed assessments of enterprise deployments, as well as produce aggregate reports of configuration security posture across such environments. CIS-CAT is available to Security Benchmarks members.

Throughout 2015 we added 30 Open Vulnerability and Assessment Language (OVAL®) tests to CIS-CAT's capabilities, for a total of 120, thus increasing the technologies it covers from 53 Benchmarks at the beginning of the year to 73 by the end of December. Beyond increasing coverage, a major feature for automatic assessment was added to CIS-CAT. With this capability, CIS-CAT is able to automatically examine the target endpoint, identify the applicable Benchmarks, and run the assessment for each.



CIS OVAL Repository

In September 2015, CIS became the conservator of the official OVAL repository and the OVAL language. The OVAL repository is a community-driven set of OVAL inventory, vulnerability, configuration, and definitions used to standardize the assessment and reporting of the machine state of computer systems.

CIS worked with the OVAL community at large to collaboratively establish a GitHub® repository and a fronting website hosted in Amazon Web Services®, while working with the DHS to negotiate appropriate licensing.

The importance of the OVAL repository is stated most aptly in terms of how it supports security programs' day-to-day operations: Without the OVAL repository, many software vulnerabilities would go unchecked and enterprises around the world would be far less secure than they are today.

Prior to becoming CIS members, we were manually auditing our systems using the free PDF version of the Benchmarks. This turned out to be a long and time-consuming process taking several days to manually audit a system. After joining CIS, we are now using the CIS-CAT audit tool. The automated process takes just a few minutes for each system to scan, allowing us to run regular scans to quickly identify any system changes that affect security hardening. We are in the process of automating CIS-CAT audits for every system connected to our networks, including production servers, user workstations, and laptops.

MICHAEL BUSINGER

CISSP, GPEN, GCIH, CEH, Sr. Security Engineer, Zix Corporation

CIS Product Certifications

CIS Certified Security Software Products are those that are tested and certified by CIS to accurately measure and report conformity of system configurations with the technical settings defined in the CIS Security Benchmarks. CIS Security Software members can use the "CIS Certified" logo to demonstrate a strong commitment to consensus-based configuration security recommendations.

In 2015, the number of members awarded CIS product certifications increased by 19%.



CIS Prog. Mgr. Shevaun Culmer-Reid prepares to discuss Security Benchmarks at the Large Installation System Administration (LISA) conference in Washington, D.C.



Alan Paller,
CIS Co-Founder and
Board Member

CIS Amazon Machine Images (AMIs) in Amazon Web Services (AWS) Marketplace

We worked throughout the year to bring the concept of our member Amazon Machine Images (AMIs) to the Amazon Marketplace, so that nonmembers can take advantage of “start secure” instances for a per-compute-hour charge.

During the second half of 2015, the security automation team was able to create a repeatable and automated process to produce member AMIs as updates were required or new Benchmarks were completed. Use of the AMIs in the commercial marketplace started to take hold in Q4.

Member AMIs are now on an automated lifecycle that aligns with our members’ automated provisioning expectations in a Development Operations environment. We now have 10 AMIs in the Amazon Marketplace.

In conjunction with this, we have been working to establish a presence in Amazon’s AWS GovCloud and Intelligence Cloud (IC) regions.

A Sampling of Security Benchmarks Members





CIS CRITICAL SECURITY CONTROLS

Overview

Over the past year, CIS successfully integrated the work of the Council on CyberSecurity and its programs on the Critical Security Controls (CIS Controls). The goal of the integration was to provide the infrastructure needed for a more mature and organized program to better maintain the currency of the CIS Controls.

CIS Controls are a set of internationally recognized measures that form the foundation of basic cyber hygiene demonstrated to prevent 80–90% of all known attacks. The CIS Controls were conceived at the National Security Agency in 2008 under the guidance of Tony Sager. They are developed and maintained by an international consortium of expert volunteers who apply real-world experience to their development.

The integration also offered an opportunity to brand the Critical Security Controls as the CIS Controls, with a new logo and webpage. The CIS Controls program is now positioned to take a major step toward broader adoption in 2016.

The CIS Controls team pursued the goals of: updating CIS Controls to Version 6.0, measurably increasing adoption and use of CIS Controls, and building an expanded ecosystem of complementary tools to support wider uptake of CIS Controls.

CIS Critical Security Controls Version 6.0

The CIS Controls update involved collecting and processing feedback from the technical community, managing panels of volunteers who integrated the comments into the new version, and, for the first time since the inception of CIS Controls, measurement guidance to ensure effective implementation. In July, the team facilitated a public call for comment and launched a media campaign to raise awareness. The final version was published in October.



CIS Sr. V.P. of Programs Kathleen Patentreger, and Brig. Gen., USAF (Ret.) Steven J. Spano, CIS President & COO, at a CIS Controls event in Washington, D.C.

CIS Controls Companion Guides

In parallel with the Version 6.0 update, the panel members initiated the creation of several new smaller companion products on topics such as measuring CIS Controls, mobile security, privacy, and the Internet of Things. All of these are significant in their own right, though the measurement guide will provide users with thresholds to assess their implementation progress. This collection will be continually expanded with new guides in 2016 to include home networking, small and medium-sized business, and more.

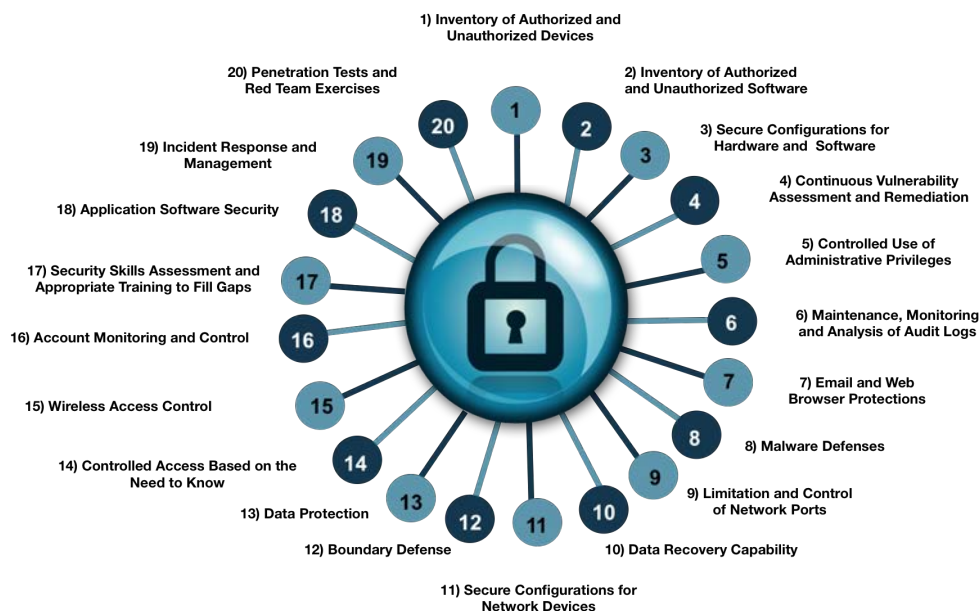
Champion Commercial License

The Champion License is for organizations and individuals who use CIS Controls commercially for the purpose of auditing, consulting, security assessments, training, and tool development, for example. (Non-commercial users are still allowed free access to CIS Controls.) The Champion License is priced based on the size of an organization's revenue, and offers the use of a Champion logo for the company's marketing purposes, acknowledgment on the CIS website, and participation in a semi-annual webcast on security topics. The first Champion License application was received by the end of December. CIS has established the Champion License to assist in the support of ongoing costs of updating and maintaining the CIS Controls and assorted tools such as the Companion Guides.



CIS Sr. V.P. & Chief Evangelist Tony Sager talks about CIS Controls.

Top 20 CIS Critical Security Controls





CIS Sr. V.P. Tony Sager and an attendee at a CIS Controls event in Washington, D.C.

Community Attack Model

CIS Controls have always been based on knowledge of the threat, with the understanding that offense (what the bad guys are doing) must inform defense (how our cyber defenders respond). Initially the CIS Controls were mapped to a set of commonly known threats, and to take it a step further, we worked with the creators of the most authoritative threat reports, like Verizon, to map our CIS Controls to their findings. We have since established relationships with other major threat vendors to continue the process, and these mappings will be made available to the public. We are also developing an attack model process that will help the community align its security strategy around the most relevant threats in an organized framework.

By the Numbers

- Completed Version 6.0 of CIS Controls
 - More than 3,000 downloads in the first week; 13,844 by the end of December 2015
- Supported launch event 16 October, with 936 simulcast registrations and 101 on-site participants
- Created four new companion documents focusing on:
 - Measurement
 - Privacy
 - Internet of Things
 - Mobile devices



James and Kelli Tarala, subject matter expert contributors to CIS Controls

INTEGRATED INTELLIGENCE CENTER

The operations core of CIS is our Integrated Intelligence Center (IIC). The IIC serves as an important resource to facilitate collaboration across multiple levels of government (federal, state, local, tribal, and territorial), and relevant domains (both cyber and physical) to improve the responsiveness and efficiency of anticipating and responding to cyber events. The IIC is the U.S. Department of Homeland Security (DHS)-recognized resource for collaborative cyber information sharing and analysis among SLTT governments and fusion centers, and is a key cyber intelligence resource for the National Governors Association’s Governors Homeland Security Advisors Council (GHSAC).

The IIC includes the following functional areas, all working side-by-side to put the pieces of the puzzle together and identify patterns that may not have been detected without this collaborative environment:

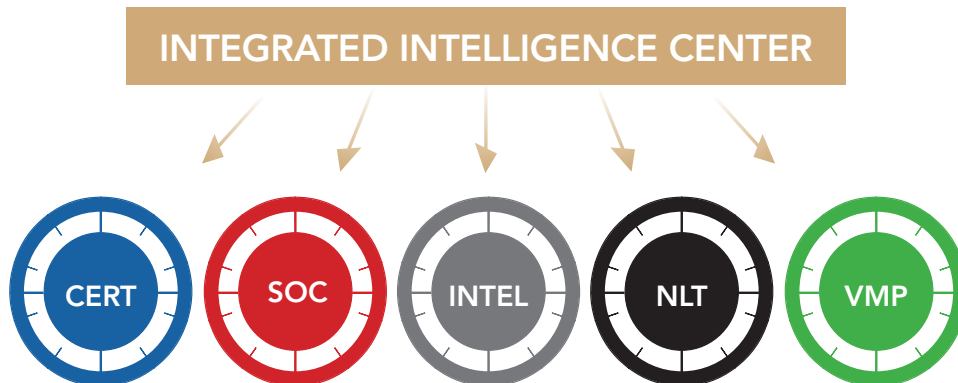
Computer Emergency Response Team (CERT) provides SLTT governments with malware analysis, computer and network forensics, malicious code analysis mitigation, and incident response.

Security Operations Center (SOC) provides 24/7/365 monitoring of cybersecurity threats and attacks that could impact SLTT governments.

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.



Computer Emergency Response Team

Response and Recovery

The CIS CERT team is a dedicated team available to assist with malware and log analysis, digital forensics, code analysis, and mitigation recommendations. In 2015 CERT handled 164 incidents, of which a majority focused on ransomware, compromised servers, and malware infections. The volume of incident response we provided to our partners increased by nearly 10% over 2014.

Key Incident Response Activities

RANSOMWARE

Ransomware made up the largest subset of CERT cases, resulting in 45 incidents investigated by CERT in 2015. Once a system becomes compromised with ransomware, the malware will encrypt all of the documents on the victim's computer as well as on any network share the system has access to. Once encrypted, the attackers will then demand a payment, usually between \$200 and \$1,000, in order to decrypt the files. Two of the most common ways entities were compromised were malicious advertisements being hosted on popular websites as well as phishing emails. Fortunately, many of the organizations have backups of their files and are able to restore them once the infection has been remediated.

COMPROMISED SERVERS

The next largest category of incident that CERT responded to was compromised servers, with 20 incidents in 2015. The majority of these systems were public facing Web servers compromised through the exploitation of out-of-date software. Vulnerable/out-of-date content management systems (CMSs) and vulnerable Web applications were popular means of compromising servers.

ADVANCED PERSISTENT THREAT (APT)

CERT responded to 18 incidents related to Advanced Persistent Threats (APTs), commonly affiliated with nation-state activity, which included a variety of system and server compromises. As in many cases CERT responds to, indicators of compromise were extracted, historical data was analyzed for similar activity, and the indicators were added to the CIS network monitoring system.

MALWARE INFECTIONS

CERT responded to 10 other incidents that occurred due to malware infections. The methods by which entities were infected included drive-by downloads that exploited a vulnerability in out-of-date software running on the victim's workstation, as well as phishing emails containing malicious links and/or attachments.

Security Operations Center

Detection and Prevention

Through its 24/7/365 SOC, CIS offers a number of services aimed at reducing risk to the nation's SLTT government cyber domain. The SOC provides network monitoring, along with threat and vulnerability analysis and notifications to SLTT governments, providing them with an enhanced ability to detect and defend against the latest cyber threats. Through its monitoring services, the SOC analyzed more than three trillion records in 2015, resulting in over 40,000 notifications.

In 2015, CIS, in partnership with DHS, continued expansion of its monitoring services, with 38 states, 24 local governments, and two territories using the services as of the end of the year. This expanded view helps inform the overall threat landscape and enables CIS to better assist all SLTT governments with threat and mitigation resources. Efforts will continue throughout 2016 to engage additional SLTT governments in monitoring as part of a comprehensive strategy for improving our collective cybersecurity posture.

CIS Network Monitoring Services

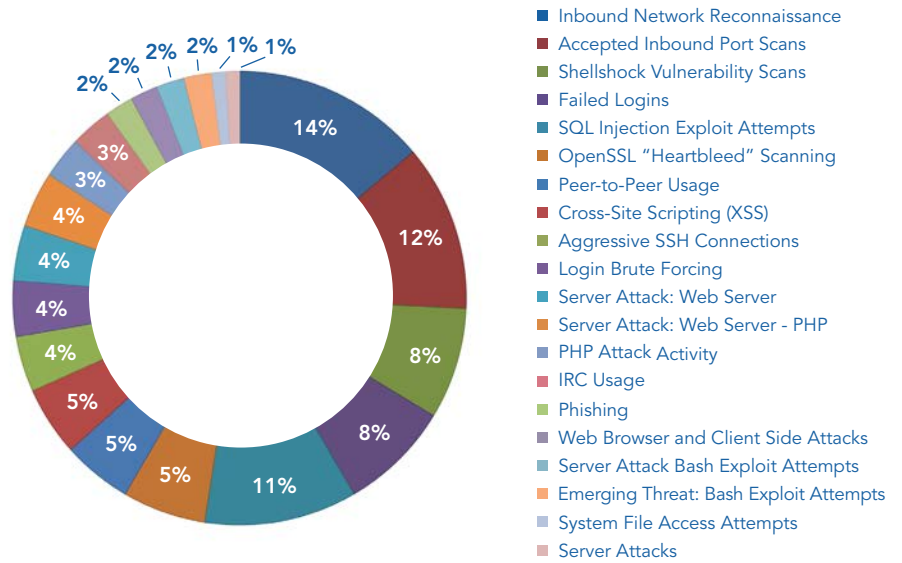
CIS network monitoring includes 24/7/365 monitoring and/or management of security devices such as firewalls, intrusion detection/prevention systems, Web gateways, and proxy devices. These services provide a view of system and network activity that allows CIS to enhance the situational awareness of SLTT government networks across the country. The SOC is able to analyze enormous amounts of data and call out the issues specific to the SLTT environment, thus saving members time and resources, and eliminating their need to respond to non-events, such as false positives.

During 2015 nearly 40% of the network attack activity tracked through CIS network monitoring consisted of scanning activity such as inbound port scans and network reconnaissance, or probing for the Shellshock and Heartbleed vulnerabilities. Inbound scanning and probes accounted for 87% of network attack activity.

The IIC issues advisories and alerts to SLTT government partners and stakeholders, and also makes them available to the public online as appropriate. These advisories include customized risk ratings for government, businesses, and home users.

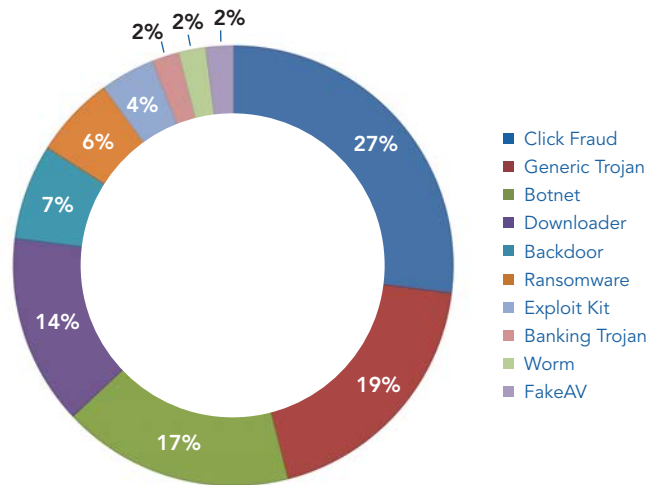


2015 Top 20 Network Attacks



Just over one-quarter of the malware infections the SOC observed as part of the CIS network monitoring during 2015 was click fraud malware, which has seen a resurgence powered by the strength of the Angler Exploit Kit (EK), making up the single largest type of malware. Generic Trojan Horse infections, which are typically designed to steal passwords or other sensitive information, made up the second largest category at 19% of all malware notifications. The most prevalent single malware was the Upatre downloader, which usually downloads the Dyre Banking Trojan to steal financial account login information.

2015 Top 10 Malware Notifications



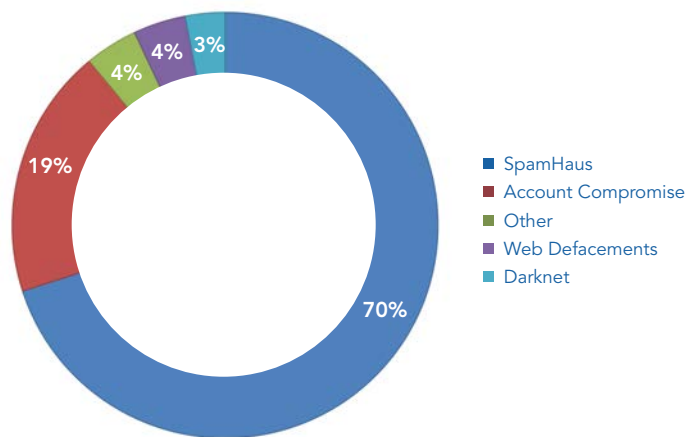
More than 40,000 actionable events were reported in 2015 from activity detected through the CIS network monitoring service, with the majority resulting from click fraud malware, generic Trojans, and botnet malware. The top 10 types of malware accounted for 80% of all monitoring notifications in 2015.

This information provides a view of system and network activity that enhances situational awareness of SLTT government networks across the country. The CIS SLTT government situational awareness contributes to the national cyber situational awareness assessment prepared by the NCCIC. It enables more timely cyber incident identification and response while providing more data for developing and implementing appropriate mitigation strategies tailored specifically to SLTT government cyber resources.

Threat and Vulnerability Notifications

In addition to the notices generated by the network monitoring, CIS provides proactive analysis of open-source data and information from trusted third parties to identify threats and vulnerabilities impacting SLTT governments. During 2015, the SOC issued more than 26,500 notices to SLTT governments, a 90% increase in volume in 2015. The majority of activity resulted from compromised system notifications and account compromises that were identified through our research activities. In particular, CIS observed a significant increase in the number of data dumps containing compromised account credentials.

2015 CIS Threat and Vulnerability Notifications



In 2015, CIS access to information from trusted third parties resulted in the distribution of 18,664 notifications to 757 members with infected systems. Over the course of 2015, CIS observed tremendous response from members with notifications of more than 12,700 non-unique infected hosts in January declining to 4,291 in December, suggesting remediation of infected systems.

In 2015, CIS began notifying website hosting providers of malicious domains hosted on their service. Once notified by CIS, the hosting providers investigate the suspected malicious domains and take them down if they find that they violate the hosting provider's terms of use. While this does not prevent the cyber threat actors from standing up another domain to host their command and control infrastructure, it does force them to do so in order to continue their malware operations.



Intel Analysis Team

Intel collects cyber threat information, evaluates it in the context of its source and reliability, analyzes it in combination with other information, and

Throughout 2015 Intel expanded its support as the key source of cyber threat intelligence including:

- 24/7/365 on-call support and situational awareness for MS-ISAC members, fusion centers, and IIC partners
- Publication of more than 77 intelligence products, including several joint products with fusion centers and DHS, and 74 Intelligence Information Reports (IIRs) disseminated to the U.S. Intelligence Community through DHS
- Presentations provided at 15 conferences and site visits with statistical support provided for more than 20 other fusion center and SLTT events
- Assistance with the DHS Fusion Center Cyber Analyst Training Course
- Cooperative efforts with the International Association of Chiefs of Police (IACP) and the Police Executive Research Forum (PERF)

disseminates actionable strategic, tactical, and operational intelligence for the nation's SLTT governments, including all 78 DHS-recognized fusion centers. Intel combines rigorous intelligence analysis standards with the easily understood and highly actionable CIS format to provide incident, pattern, and actor tracking from an unbiased, timely perspective. Source information is drawn from federal and SLTT governments, fusion centers, law enforcement agencies, trusted third parties, other information sharing and analysis centers (ISACs), and open source reporting.

2015 Cyber Threat Actor and Group Activity

Intel produced analytical reports regarding many of the most prevalent actors and campaigns that targeted SLTT governments in 2015. Widely recognized as an authoritative source of information, the shared reports

provided additional context for the victims and ensured that all federal and SLTT entities received consistent, unbiased intelligence regarding cyber threat actor and group¹ tactics, techniques, and procedures (TTPs) throughout the country.

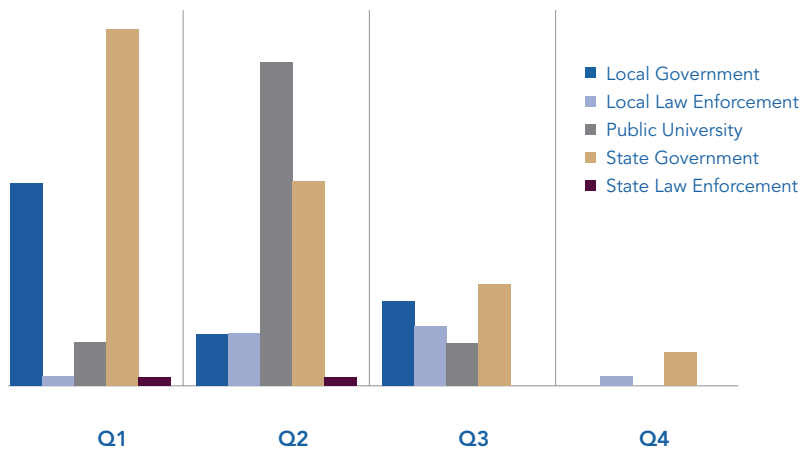
In 2015 Intel sent more than 260 incident notifications to MS-ISAC members and fusion centers about cyber threat actors and groups targeting or claiming to target SLTT governments with operational campaigns. The majority of cyber threat actor attacks against SLTT governments stemmed from a desire for recognition and attention. However, hacktivists were responsible for multiple incidents, primarily targeting local law enforcement agencies in response to incidents involving the alleged use of excessive force by a law enforcement officer.

2015 Trend and Pattern Analysis

Analysis by the Intel team identified and reported on a variety of malware and TTP patterns throughout the year. The reports furthered intelligence sharing among the federal and SLTT community, and enabled network owners and operators to receive fact-based intelligence regarding changes in the threat environment along with proactive, actionable recommendations to protect their networks.

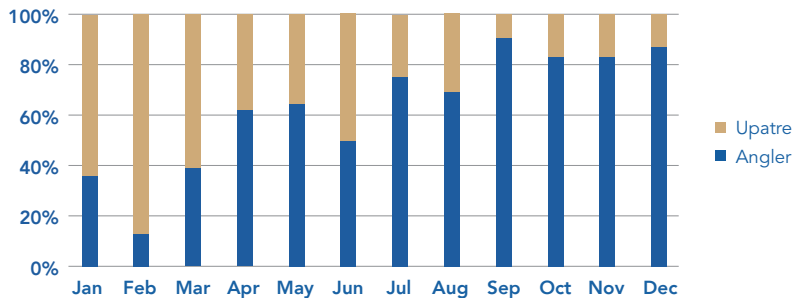
¹ A cyber threat actor is an identifiable individual person who participates in malicious cyber activity and without claiming activity in the name of one cyber threat actor group or movement. A cyber threat actor group is an identifiable group of cyber threat actors who claim allegiance to a group or organization that participates in malicious cyber activity.

2015 Cyber Threat Actor Incidents by Quarter and Targeted Entity



One of the most striking trends observed by Intel was the continued ebb and flow among different malware packages and exploit kits, particularly the decline of the Upatre downloader and the rise of the Angler EK. Upatre has been an on-again, off-again favorite of cyber criminals, as they use it to disseminate ransomware, Zeus, and Kuluoz/Asprox. As the chart below illustrates, at the beginning of 2015 Upatre and associated infections were a significant threat to SLTT governments. In April, Angler infections surpassed Upatre infections, and after June it was clear that cyber criminals favored Angler. Intel believes this is partly due to Angler’s use of malvertising as an infection vector and quick adoption of exploits.

2015 Comparison of the Percentages of Upatre and Angler Related Infections



Supporting National Intelligence

In support of national cyber intelligence requirements, Intel provided cyber threat information to the DHS Office of Intelligence and Analysis (I&A), which regularly incorporated this information in its production and threat briefing process, as well as in more than 74 Intelligence Information Reports (IIRs). The information consistently received excellent evaluations from Homeland Security, law enforcement, and U.S. Intelligence Community consumers, reflecting the high value of CIS information.





MS-ISAC V.P. of Operations Brian Calkin and, foreground, CIS V.P. of Policy & Outreach Brian de Vallance

Intel Training and Collaboration Activities

Intel continues to support the Cyber Threat Intelligence Coordination Group (CTICG) and the DHS Fusion Center Cyber Analyst Training Course. CTICG began in 2010 as a way to coordinate information sharing among SLTT and law enforcement agencies, and meets monthly via WebEx to discuss current cyber threats. The DHS Fusion Center Cyber Analyst Training Course is a weeklong training effort to provide fusion center analysts with a baseline concept of cybersecurity and the cyber threat environment.

Fusion Center Cyber Pilot

On behalf of DHS and the Office of the Director of National Intelligence (ODNI), Intel managed the Fusion Center Cyber Pilot (FC Pilot), which concluded in May 2015 with the publication of “Cyber Integration for Fusion Centers: An Appendix to the Baseline Capabilities for State and Major Urban Area Fusion Centers” and a compatible toolkit. It was coordinated with six partner fusion centers and six partner organizations, with the goal of creating a standardized, achievable, and scalable framework for all fusion centers to use in creating or advancing their own cyber programs. The Appendix to the Baseline Capabilities is available on the CIS website [here](#).

National Liaison Team

CIS has staff assigned to the National Cybersecurity and Communications Integration Center (NCCIC), a 24/7 operations coordinating center for U.S. cyber security efforts established by DHS. CIS’ NCCIC liaisons work closely with all of the NCCIC partners in both the public and private sectors. Through this resource the liaisons are able to directly share information regarding threats to SLTTs with the federal government and share federal government information with SLTT governments. CIS intelligence provided to the federal government includes daily, weekly, and monthly information on the cyber activity impacting SLTTs.

Vulnerability Management Program

The CIS Vulnerability Management Program (VMP) provides SLTT governments with vulnerability assessments, phishing engagements, penetration testing, and Web profiling.

In April 2015, CIS VMP created a new service, which identifies SLTT systems that are running out-of-date software, utilizing a Web profiling tool. The profiler is designed to connect with domains provided by members to collect data on server software and other installed Web applications, identifying version information. Using the identified version information, CIS vulnerability analysts confirm whether or not the systems are fully patched or using the most current available version. Members receive a monthly notification of potentially vulnerable systems. Since the beginning of the program in April 2015, CIS has issued 4,657 notifications to SLTTs with potentially vulnerable systems. There are currently over 22,500 domains registered for profiling.

MULTI-STATE INFORMATION SHARING & ANALYSIS CENTER

CIS is home to the MS-ISAC, one of the longest-standing national ISACs. The MS-ISAC, which includes representation by state Chief Information Security Officers or their equivalents, Chief Information Officers, local governments, tribal entities, and U.S. territories, is designated by the DHS as a key resource for cyber threat protection, response, and recovery for the nation's SLTT governments.



Bringing SLTT Government Professionals Together

The MS-ISAC has fostered a trusted environment between and among its SLTT government partners and with DHS. CIS conducts monthly MS-ISAC membership meetings via webcast 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.

The MS-ISAC works closely with other organizations to continue to build trusted relationships to further enhance the cybersecurity posture of the nation. Such 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 ISACs through the National Council of ISACs.

The Annual Meeting is the cornerstone MS-ISAC event each year, focused on deliverable-oriented working sessions that address specific areas of the MS-ISAC's objectives, with the ultimate goal to enhance our overall cybersecurity posture by working collectively.

Our largest-attended Annual Meeting to date was in 2015, with 328 attendees representing all 50 states, three tribal entities, 78 local governments, and 67 fusion centers.



2015 MS-ISAC Annual Meeting attendees

Membership in the MS-ISAC grew by 31% in 2015 to a total of 902, representing all 50 states, 832 local governments, five U.S. territories, and 15 tribal entities.



Providing 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. CIS achieves this 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 2015 from all 50 states, several U.S. territories, and 19 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

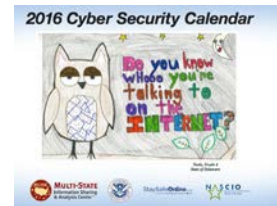
Each October, CIS serves as a co-host with DHS, the National Association of State Chief Information Officers, and the National Cyber Security Alliance in promoting National Cyber Security Awareness Month (NCSAM). CIS develops and distributes Cybersecurity Awareness toolkit materials to all MS-ISAC members in support of Awareness Month. The goal is to promote a consistent message about cybersecurity education and awareness and to provide products for broad distribution.

The materials include posters, bookmarks, calendars, and other awareness materials. These materials are branded so that each MS-ISAC member can customize them with its own logo and website. CIS also makes this information available to the public online at www.msisac.org.

CIS 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 2015, 48 state governors issued proclamations or letters of support, along with two U.S. territory and 35 local government officials.

National Kids Safe Online Poster Contest

One of our 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 them 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. In 2015, 12 states participated in the contest.



National Best of the Web Contest

CIS conducted its seventh annual Best of the Web contest in 2015 to recognize state, local, and territorial governments that use websites to promote cybersecurity.



State Government Winner 2015
State of Delaware



Local Government Winner 2015
Johnson County, Kansas



2015 MS-ISAC ANNUAL MEETING



- ① MS-ISAC member Arnold Kishi from Hawaii, MS-ISAC V.P. of Partner Engagement Mike Aliperti, MS-ISAC member Lynne Pizzini from Montana, and MS-ISAC Sr. V.P. of Operations and Chair Thomas Duffy
- ② MS-ISAC member John Essner from New Jersey and MS-ISAC Program Specialist Erin Dayton
- ③ DHS Program Lead Erin Meehan, MS-ISAC V.P. Mike Aliperti, and MS-ISAC Dir. of Stakeholder Engagement Andrew Dolan

- ④ MS-ISAC members Chuck Scharnagle from the Mohegan Tribe of Indians and Dr. Robert Pittman of Los Angeles County
- ⑤ MS-ISAC Mgr. of Security Operations Stacey Wright addresses MS-ISAC members.
- ⑥ Left to right, MS-ISAC members David Whicker and Maria Thomas from North Carolina with MS-ISAC member James Stoner from Colorado

Nationwide Cyber Security Review

The Nationwide Cyber Security Review (NCSR) is an annual voluntary self-assessment survey designed to evaluate cybersecurity management 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 an organization's operations.



DHS partnered with CIS, along with NASCIO and NACo, to develop and conduct the Review, which took place for the fourth time in 2015. 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 2015 NCSR included all 50 states, 55 local governments, and more than 260 state agencies, 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 allows each organization to establish their own baseline and also helps identify priority areas by understanding how their own security posture compares with that of their peers.

The 2015 NCSR represents a first step for the SLTT community to collaboratively adopt the principles of the Framework. Through developing a baseline of cybersecurity maturity using the NCSR, the MS-ISAC partner community can come together and identify 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.

Using the results from the 2015 NCSR, MS-ISAC will be working with DHS to create a Congressional Summary Report detailing the current cybersecurity posture of SLTT governments.

MAKING SECURITY AFFORDABLE

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 have a negative impact on their ability to implement the security controls needed to defend against the ever-increasing cybersecurity threats.

In 2015 the CIS Trusted Purchasing Alliance entered its fourth year. This program aggregates the purchasing power of the public sector to allow all participants the ability to improve their cybersecurity posture at a lower cost than they could achieve individually.

Product and service choices for the aggregate buys are driven by the positive impact on cybersecurity infrastructure and customer needs. CIS oversees a review board of government partners to carefully review and select potential offerings, and then works with the vendor community to negotiate volume discount purchasing opportunities.

During 2015, 320 entities took advantage of aggregate buy opportunities, an increase of nearly 13% from 2014. In total, more than \$8 million in cost savings were achieved in 2015 through the CIS Trusted Purchasing Alliance.



CIS IN THE SPOTLIGHT

- CIS CEO Jane Holl Lute briefed the governors at the National Governors Association's (NGA) 2015 annual summer meeting and worked with NGA senior staff to plan their cyber policy academy; and two senior CIS officials participated in separate NGA cyber webinars for governors' chiefs of staff, state chief information officers, and key cyber and IT policy advisors.



MS-ISAC V.P. Brian Calkin, Congressman Paul D. Tonko (D-NY), CIS President and COO Steven J. Spano, and CIS Chief Administrative Officer Richard J. Licht

- CIS CEO Jane Holl Lute addressed a caucus of the U.S. Senate on cybersecurity issues.
- CIS senior staff provided technical assistance for the U.S. Senate's information sharing legislation.
- CIS staff continued to provide input to various national think tanks on cybersecurity projects.
- CIS staff continued engagement with leadership of national law enforcement associations, and provided input in an upcoming state and local law enforcement cyber guide.

CIS CARES

CIS Cares is our employee volunteer program dedicated to supporting community causes. Employees donate their time and money to local and national charities throughout the year. CIS Cares-sponsored events and charity activities in 2015 included:

- Regional Food Bank of Northeastern New York
- National Breast Cancer Foundation
- New York State Troopers Police Benevolent Association
- East Greenbush (N.Y.) Miracle League
- Holiday Adopt-a-Family program in Albany and Rensselaer counties

FINANCIALS

STATEMENTS OF FINANCIAL POSITION

	YEARS ENDED DECEMBER 31,	
	2015	2014
ASSETS		
Cash	\$ 7,961,238	\$ 6,757,490
Accounts receivable.....	1,731,140	1,038,440
Unbilled receivables	105,650	92,671
Prepaid expenses and other assets.....	402,270	248,722
Leasehold improvements and equipment, net.....	1,647,221	1,723,424
Total assets.....	\$11,847,519	\$9,860,747
LIABILITIES		
Accounts payable.....	\$ 360,510	\$ 607,884
Accrued expenses.....	741,402	706,597
Deferred revenue	4,033,917	3,026,353
	5,135,829	4,340,834
COMMITMENTS AND CONTINGENCIES		
Net assets, unrestricted.....	\$ 6,711,690	\$ 5,519,913
TOTAL LIABILITIES AND NET ASSETS.....	\$ 11,847,519	\$ 9,860,747

STATEMENTS OF CASH FLOW

	YEARS ENDED DECEMBER 31,	
	2015	2014
CASH FLOWS PROVIDED (USED) BY OPERATING ACTIVITIES		
Increase in unrestricted net assets.....	\$ 1,191,777	\$ 1,474,709
Adjustments to reconcile increase in unrestricted net assets to net cash provided (used) by operating activities		
Depreciation.....	519,282	403,095
Unrealized loss on investment in Cyber Griffin, Inc.....	—	550,000
(Increase) decrease in		
Accounts receivable.....	(692,700)	296,187
Unbilled revenue.....	(12,979)	3,866
Prepaid expenses and other assets.....	(153,548)	(21,718)
(Increase) decrease in		
Accounts payable.....	(247,374)	(101,384)
Accrued expenses.....	34,805	320,122
Deferred revenue.....	1,007,564	1,008,534
	1,646,827	3,933,411
CASH FLOWS PROVIDED (USED) BY INVESTING ACTIVITIES		
Purchase of leasehold improvements and equipment	\$ (443,079)	\$ (669,481)
Net increase in cash.....	1,203,748	3,263,930
CASH (beginning of year).....	\$ 6,757,490	\$ 3,493,560
CASH (end of year).....	\$ 7,961,238	\$ 6,757,490
SUPPLEMENTARY CASH FLOW INFORMATION		
Cash paid during the year for Income taxes.....	\$ 2,605	\$ 4,812

STATEMENTS OF ACTIVITIES

	YEARS ENDED DECEMBER 31,	
	2015	2014
REVENUES AND OTHER SUPPORT		
Membership dues.....	\$ 4,246,825	\$ 3,225,813
Cooperative agreement.....	10,553,492	9,508,911
Managed security services.....	2,846,820	3,164,048
Aggregate purchasing.....	649,728	573,474
Contributions.....	437,004	85,894
Consulting and other revenue.....	805,154	283,585
Interest income.....	24,167	23,167
Total revenues and other support.....	\$19,563,190	\$16,864,892
EXPENSES		
Salaries and wages.....	\$ 9,731,189	\$ 7,234,953
Payroll taxes.....	685,542	542,653
Employee benefits.....	1,048,433	980,532
Contributions.....	225,330	—
Depreciation.....	519,282	403,095
Information technology and security services.....	3,047,237	3,429,799
Insurance.....	105,473	75,684
Marketing and communication services.....	179,818	143,150
Occupancy.....	536,414	570,274
Professional and other consulting fees.....	340,199	88,570
Office, computer equipment, and licenses.....	841,070	622,525
Supplies, postage, printing, and miscellaneous.....	309,143	225,620
Travel.....	801,510	520,987
Total expenses.....	\$ 18,370,640	\$ 14,837,842
Change in unrestricted net assets from operations	\$ 1,192,550	\$ 2,027,050
NON-OPERATING LOSS		
Unrealized loss on investment in Cyber Griffin, Inc.....	—	\$ 550,000
Change in unrestricted net assets from operations before provision for income taxes.....	\$ 1,192,550	\$ 1,477,050
PROVISION FOR INCOME TAXES.....	\$ 773	\$ 2,341
Change in unrestricted net assets.....	\$ 1,191,777	\$ 1,474,709
NET ASSETS (unrestricted, beginning of year).....	\$ 5,519,913	\$ 4,045,204
NET ASSETS (unrestricted, end of year).....	\$ 6,711,690	\$ 5,519,913

CIS Leadership

OFFICERS AND BOARD OF DIRECTORS

Officers

Jack Arthur, Treasurer
Executive Vice President
Octo Consulting Group

Jane Holl Lute
Chief Executive Officer
Center for Internet Security

Deirdre O'Callaghan
Secretary and Chief Counsel
Center for Internet Security

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

Directors

John M. Gilligan, Chairman
President and COO
Schafer Corporation

Michael Assante
ICS Director
SANS Institute

Dr. Ramon Barquin
President and CEO
Barquin International

Karen S. Evans
Partner
KE&T Partners, LLC

Maureen O. Helmer
Partner
Barclay Damon, LLP

Clint Kreitner
Founding President and Former CEO
Center for Internet Security

Bruce Moulton
Vice President, Information Technology
National Grand Bank

Alan Paller
Founder and Director of Research
SANS Institute

Franklin Reeder
Co-Founder
Center for Internet Security

Phil Venables
Managing Director and
Chief Information Risk Officer
Goldman Sachs & Co.

EXECUTIVE TEAM

Kerry Coffey
Senior Vice President
Business Development

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

Laura Iwan
Chief Information Security Officer

Richard J. Licht
Chief Administrative Officer

Kathleen Patentreger
Senior Vice President of Programs

Tony Sager
Senior Vice President and
Chief Evangelist

Rick Stegmann
Chief Information Officer

Albert Szesnat
Chief Financial Officer

2015 LEADERSHIP TRANSITIONS

In January 2015, the Council on CyberSecurity and the Center for Internet Security joined forces to integrate their respective programs providing national and global leadership in cybersecurity. Former CIS President and CEO William F. Pelgrin was named co-CEO along with Jane Holl Lute, the former President and CEO of the Council on CyberSecurity.

Pelgrin retired from CIS in June 2015, and continued to serve on the CIS Board of Directors for the remainder of 2015. His storied career spanned nearly four decades and has been largely dedicated to advancing the state of cybersecurity across the world, including five years as CEO for CIS. Pelgrin left a lasting legacy at both the national as well as state and local government levels.

Pelgrin spent part of his career as New York State's first CISO, where his collaborative management approach was the impetus behind the Multi-State Information Sharing & Analysis Center (MS-ISAC). He established MS-ISAC in 2003 to provide a central resource for state and local governments to share information between and among members in order to detect, defend against, and respond to cyber threats. Thanks largely to his efforts, and those of the team he assembled, the MS-ISAC now includes members from all 50 states, hundreds of local governments, and several U.S. territories and tribal entities.

"William Pelgrin's outstanding vision and commitment have elevated CIS on the national and international stages as a trusted leader in cybersecurity, and he has positioned CIS to be responsive to the ever-changing security threat landscape," said John M. Gilligan, Chairman of the CIS Board of Directors.

Holl Lute, former Deputy Secretary of DHS, replaced Pelgrin as CEO, while Brig. Gen., USAF (Ret.) Steven J. Spano was named President and COO for CIS in June 2015.

Holl Lute's career includes service as an officer in the United States Army, as a Special Adviser to the Secretary General of the United Nations, and at the DHS. She served on the National Security Council supporting both President George W. Bush and President Barack Obama, and was President and CEO for the Council on CyberSecurity, a nonprofit organization.

Spano has three decades of leadership experience with the United States Air Force, where he led IT policy and operations organizations in command assignments across the globe. He retired in 2011 and joined Amazon Web Services® Worldwide Public Sector as the Director for the DoD and the National Security teams. He joined CIS in June 2015.



William F. Pelgrin
Former CIS President & CEO



Steven J. Spano
Brig. Gen., USAF (Ret.)
CIS President & COO



2015 CIS HIGHLIGHTS



- ① CIS staff at retreat at Saratoga Historical National Park
- ② Saratoga Historical National Park Battlefield Guide Jim Hughto at CIS Staff Retreat
- ③ MS-ISAC Dir. Andrew Dolan, MS-ISAC Sr. V.P. Thomas Duffy, and MS-ISAC V.P. Brian Calkin

- ④ Left to right, MS-ISAC member Elayne Starkey from Delaware and MS-ISAC member Lynne Pizzini from Montana
- ⑤ CIS CEO Jane Holl Lute
- ⑥ Left to right, Frank Lujan and Joey Manibusan, MS-ISAC members from the Territory of Guam

For more information about CIS

Contact: Barbara Ware

Director of Communications

Email: Barbara.Ware@cisecurity.org

Graphic design: Snap Line Studio (snaplinestudio.net)


Principal photography: Barbara Ware. Additional photography: Andrew Dolan




**Center for
Internet Security®**

31 Tech Valley Drive
East Greenbush, New York 12061
T. (518) 266 – 3460
F. (518) 266 – 2085
www.cisecurity.org

Follow Us on 

Find Us on 

Join Us on 

Watch Us on 