Article II

Article II - (201 - 209) INTERNET SECURITY AND PRIVACY ACT

§ 201. Short title. This article shall be known and may be cited as the "internet security and privacy act".

§ 202. Definitions. As used in this article, the following terms shall have the following meanings:

1. “Collect” shall mean to store information, including via cookie technology, for purposes of retrieval at a later time to initiate communication with or make determinations about the person who is the subject of such information.

2. “Disclose” shall mean to reveal, release, transfer, disseminate or otherwise communicate information orally, in writing or by electronic or other means, other than to the person who is the subject of such information.

3. “Internet” shall mean a system of linked computer networks, international in scope, that facilitate data transmission and exchange.

4. “Office” shall mean the state office of information technology services.

5. “Personal information” shall mean any information concerning a natural person which, because of name, number, symbol, mark or other identifier, can be used to identify that natural person.

6. "State agency" shall have the same meaning as the meaning given to "agency" under subdivision one of section ninety-two of the public officers law.

7. "State agency website" shall mean an internet website operated by or for a state agency. Such term shall include those websites operated on behalf of state agencies by other public or private entities, but shall not include any portions of the internet outside the control of the state agency.

8. "User" shall mean any natural person who uses the internet to access a state agency website.

§ 203. Model internet privacy policy.

1. The office shall adopt rules and regulations in conformity with the provisions of this article, and specify a model internet privacy policy for state agencies that maintain state agency websites. Such model privacy policy shall include, but not be limited to, the following elements:

(a) a statement of any information, including personal information, the state agency website will collect with respect to the user and the use of the information;

(b) the circumstances under which information, including personal information, collected may be disclosed;

(c) whether any information collected will be retained by the state agency, and, if so, the period of time that such information will be retained;

(d) the procedures by which a user may gain access to the collected information pertaining to that user;

(e) the means by which information is collected and whether such collection occurs actively or passively;

(f) whether the collection of information is voluntary or required, and the consequences, if any, of a refusal to provide the required information; and

(g) the steps being taken by the state agency to protect the confidentiality and integrity of the information.

2. Each state agency that maintains a state agency website shall adopt an internet privacy policy which shall, at a minimum, include the information required by the model internet privacy policy. Each state agency shall post its internet privacy policy on its website. Such posting shall include a conspicuous and direct link to such privacy policy.

3. The model internet privacy policy specified by the office shall also be made available at no charge to other public and private entities.

§ 204. Collection and disclosure of personal information. No state agency shall collect personal information concerning a user through a state agency website, or disclose personal information concerning a user to any person, firm, partnership, corporation, limited liability company or other entity, including internal staff who do not need the information in the performance of their official duties pursuant to a state agency purpose meeting the requirements of subdivision one of section two hundred six of this article, unless such user has consented to the collection or disclosure of such personal information. For the purposes of this section, the voluntary disclosure of personal information to a state agency by a user through a state agency website, whether solicited or unsolicited, shall constitute consent to the collection or disclosure of the information by the state agency for the purposes for which the user disclosed it to the state agency, as reasonably ascertainable from the nature and terms of the disclosure.

§ 205. Access to personal information. Except as otherwise provided by law, a state agency shall provide users with access to all personal information pertaining to such user which has been collected through its state agency website. Access to such personal information and the opportunity to request correction or amendment of such personal information shall be provided to users in the manner provided for access to and correction or amendment of personal information under section ninety-five of the public officers law. A state agency shall provide a user access to such personal information via the internet when such access is feasible and only if that access can be provided in a secure manner.

§ 206. Exceptions. Notwithstanding section two hundred four of this article, a state agency may collect or disclose personal information if the collection or disclosure is:

1. necessary to perform the statutory duties of the state agency that collected or is collecting the personal information, or necessary for that agency to operate a program authorized by law, or authorized by state or federal statute or regulation;

2. made pursuant to a court order or by law;

3. for the purpose of validating the identity of the user; or

4. if the information is used solely for statistical purposes and is in a form that cannot be used to identify any particular person.

§ 207. Construction. Nothing in this article shall abridge public access to information available or permitted by any other provision or rule of law, including without limitation article six of the public officers law. Nothing in this article shall authorize the collection or disclosure of information the collection or disclosure of which is prohibited or restricted by any other provision of law, including without limitation article six-A of the public officers law. Nothing in this article shall alter the obligations of state agencies and users pursuant to article six-A of the public officers law.

§ 208. Notification; person without valid authorization has acquired private information.

1. As used in this section, the following terms shall have the following meanings:

(a) "Private information" shall mean either:

(i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

(1) social security number;

(2) driver's license number or non-driver identification card number;

(3) account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account;

(4) account number, or credit or debit card number, if circumstances exist wherein such number could be used to access to an individual's financial account without additional identifying information, security code, access code, or password; or

(5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, or retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity; or

(ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account.

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(b) "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity may consider the following factors, among others:

(1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) indications that the information has been downloaded or copied; or

(3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

(c) "State entity" shall mean any state board, bureau, division, committee, commission, council, department, public authority, public benefit corporation, office or other governmental entity performing a governmental or proprietary function for the state of New York, except:

(1) the judiciary; and

(2) all cities, counties, municipalities, villages, towns, and other local agencies.

(d) "Consumer reporting agency" shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate

commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under subdivision two of this section.

2. Any state entity that owns or licenses computerized data that includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the integrity of the data system. The state entity shall consult with the state office of information technology services to determine the scope of the breach and restoration measures. Within ninety days of the notice of the breach, the office of information technology services shall deliver a report on the scope of the breach and recommendations to restore and improve the security of the system to the state entity.

(a) Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the state entity reasonably determines such exposure will not likely result in misuse of such information, or financial or emotional harm to the affected persons. Such a determination must be documented in writing and maintained for at least five years. If the incident affected over five hundred residents of New York, the state entity shall provide the written determination to the state attorney general within ten days after the determination.

(b) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under any of the following laws, nothing in this section shall require any additional notice to those affected persons, but notice still shall be provided to the state attorney general, the department of state and the office of information technology services pursuant to paragraph (a) of subdivision seven of this section and to consumer reporting agencies pursuant to paragraph (b) of subdivision seven of this section:

(i) regulations promulgated pursuant to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. 6801 to 6809), as amended from time to time;

(ii) regulations implementing the Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. parts 160 and 164), as amended from time to time, and the Health Information Technology for Economic and Clinical Health Act, as amended from time to time;

(iii) part five hundred of title twenty-three of the official compilation of codes, rules and regulations of the state of New York, as amended from time to time; or

(iv) any other data security rules and regulations of, and the statutes administered by, any official department, division, commission or agency of the federal or New York state government as such rules, regulations or statutes are interpreted by such department, division, commission or agency or by the federal or New York state courts.

3. Any state entity that maintains computerized data that includes private information which such agency does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.

5. The notice required by this section shall be directly provided to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the state entity who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;

(c) telephone notification provided that a log of each such notification is kept by the state entity who notifies affected persons; or

(d) Substitute notice, if a state entity demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) e-mail notice when such state entity has an e-mail address for the subject persons;

(2) conspicuous posting of the notice on such state entity's web site page, if such agency maintains one; and

(3) notification to major statewide media.

6. Regardless of the method by which notice is provided, such notice shall include contact information for the state entity making the notification, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

7.

(a) In the event that any New York residents are to be notified, the state entity shall notify the state attorney general, the department of state and the state office of information technology services as to the timing, content and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. Such notice shall be made without delaying notice to affected New York residents.

(b) In the event that more than five thousand New York residents are to be notified at one time, the state entity shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected New York residents.

8. The state office of information technology services shall develop, update and provide regular training to all state entities relating to best practices for the prevention of a breach of the security of the system.

9. Any covered entity required to provide notification of a breach, including breach of information that is not "private information" as defined in paragraph (a) of subdivision one of this section, to the secretary of health and human services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, as amended from time to time, shall provide such notification to the state attorney general within five business days of notifying the secretary.

10. Any entity listed in subparagraph two of paragraph (c) of subdivision one of this section shall adopt a notification policy no more than one hundred twenty days after the effective date of this section. Such entity may develop a notification policy which is consistent with this section or alternatively shall adopt a local law which is consistent with this section.

§ 209. Notification of a breach of the security of the system or a breach of network security; shared data.

1. The office shall, within twenty-four hours of either being notified of or receiving evidence of a breach of the security of the system, or a breach of network security, as defined in paragraphs (a) and (b) of subdivision three of this section, notify the chief information officer, the chief information security officer, and where appropriate, the cyber security coordinator of any state entity with which it shares data, provides networked services or shares a network connection whose data, services or connection is reasonably suspected to be affected by any such breach.

2. The office shall provide the chief information officer, the chief information security officer, and where appropriate, the cyber risk coordinator of any state entity, who has been notified pursuant to subdivision one of this section, with its plan for remediation of the breach and future protection of such data and network.

3. For purposes of this section:

(a) “Breach of the security of the system” shall have the same meaning as defined in paragraph (b) of subdivision one of section two hundred eight of this article.

(b) "Breach of network security" shall mean unauthorized access to or access without valid authorization of a computer network which compromises the security, confidentiality, or integrity of such network.

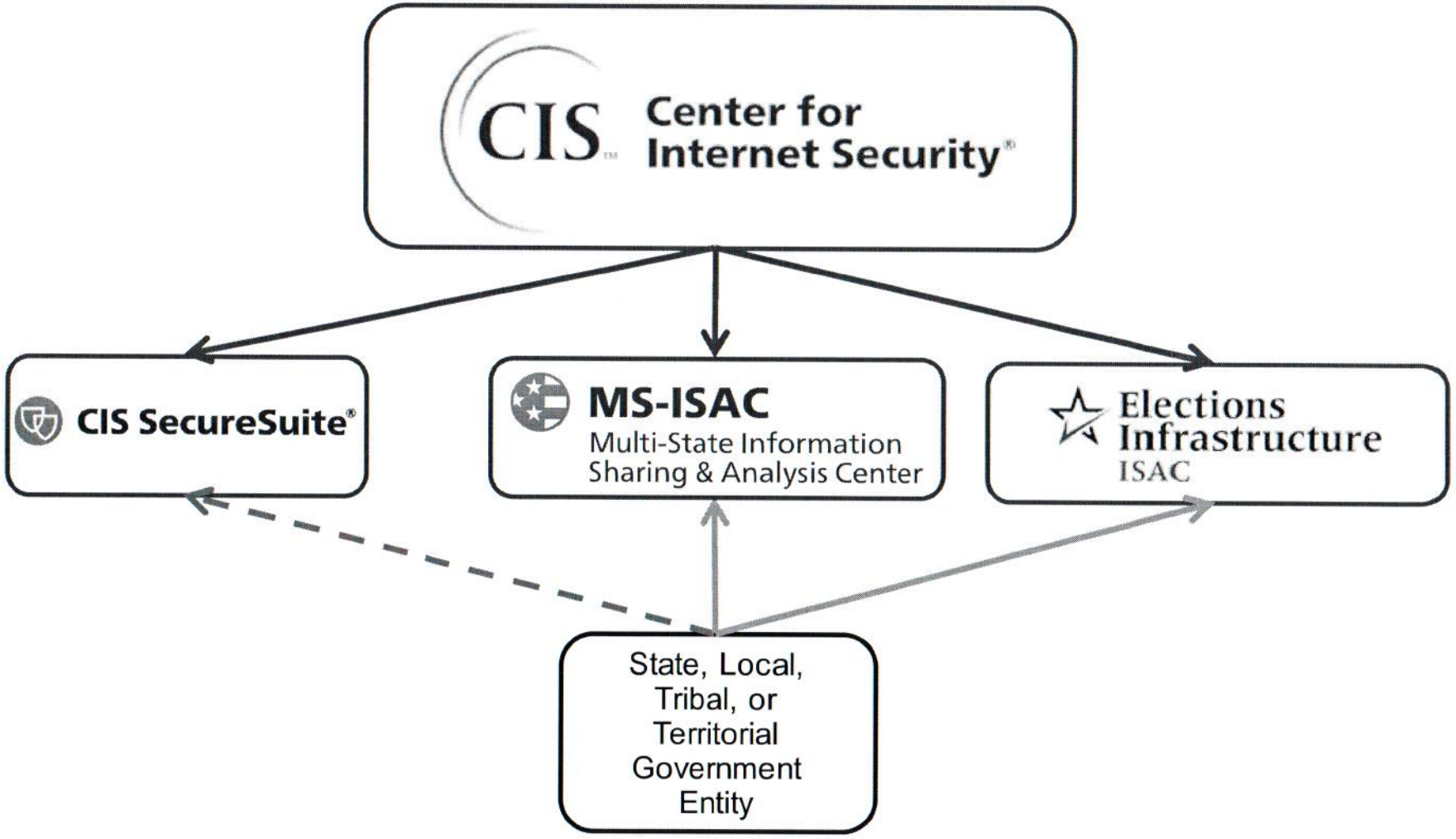
(c) "State entity" shall have the same meaning as provided by paragraph (c) of subdivision one of section two hundred eight of this article.

CIS Center for Internet Security®

MS-ISAC
Multi-State Information Sharing & Analysis Center

Cybersecurity 101

Andrew Dolan
Director of Stakeholder Engagement
MS-ISAC/EI-ISAC


CIS Center for Internet Security®
CIS SecureSuite®
MS-ISAC
Multi-State Information Sharing & Analysis Center
Elections Infrastructure ISAC
State, Local, Tribal, or Territorial Government Entity

Multi-State Information Sharing and Analysis Center

The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's SLTT governments.

TLP: WHITE

About MS-ISAC Membership

Free and Voluntary

No Mandated Information Sharing

Only Registration is Required!

To join or get more information:

https://learn.cisecurity.org/ms-isac-registration

Who We Serve

MS-ISAC Members include:

- ✓All 56 US States and Territories
- ✓All 79 federally recognized fusion centers
- ✓More than 3,000 local governments, public education entities and tribal nations

State, Local, Tribal, and Territorial

Cities, counties, towns, airports, public education, police departments, ports, transit associations & more

24 x 7 Security Operations Center

Central location to report any cybersecurity incident

- **Support:**
  - Network Monitoring Services
  - Research and Analysis
- **Analysis and Monitoring:**
  - Threats
  - Vulnerabilities
  - Attacks
- **Reporting:**
  - Cyber Alerts & Advisories
  - Web Defacements
  - Account Compromises
  - Hacktivist Notifications

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@msisac.org

Why Government?

Criminals look for data...

and governments have a lot of it!

Malware is everywhere! The Value of Stolen Information

… and the costs of a breach

Record Type	Estimated Underground Value pre record (McAfee and World Privacy Forum)
Financial Account	$14-$25
Credit/Debit Card	$4-$5
Medical Account Data	$0.03-$2.42
Full Medical Record with supporting documents	$50

Record Type	Estimated Breach Cost Per Record (Ponemon Institute 2016 Report)
Health	$355
Education	$246
Financial	$221

Website Defacements

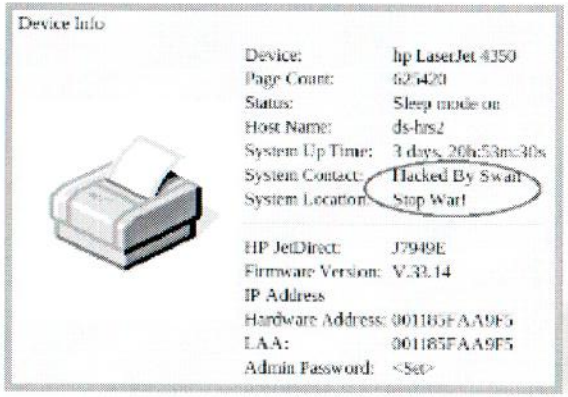
Key Website Defacement Vulnerabilities:

- Openly accessible embedded webservers
- Outdated Content Management Systems (CMS)

Identifying Web Defacements and Actors:

- Zone-H.org
- Twitter
- Facebook

ADST Website Defacement



Defaced Printer Webserver

SWATting

- Home invasion/armed robbery
- Murder/Homicide/Suicide
- Domestic violence incident
- Workplace violence incident
- Plane crash
- Bomb threat

Pranks, harassment & malicious targeting

Spoofed Phone Numbers

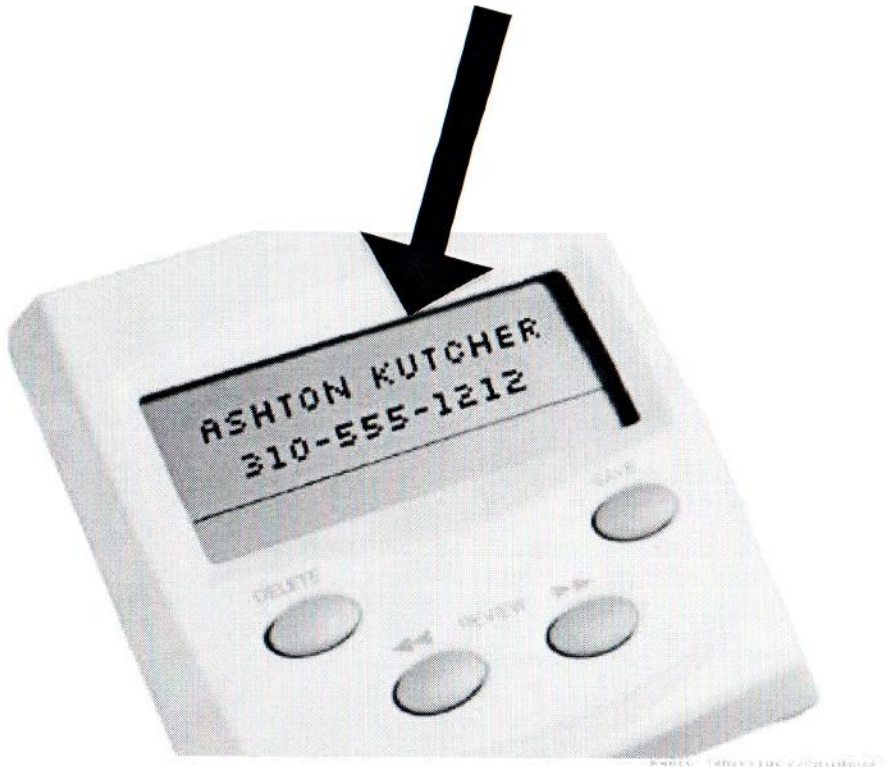
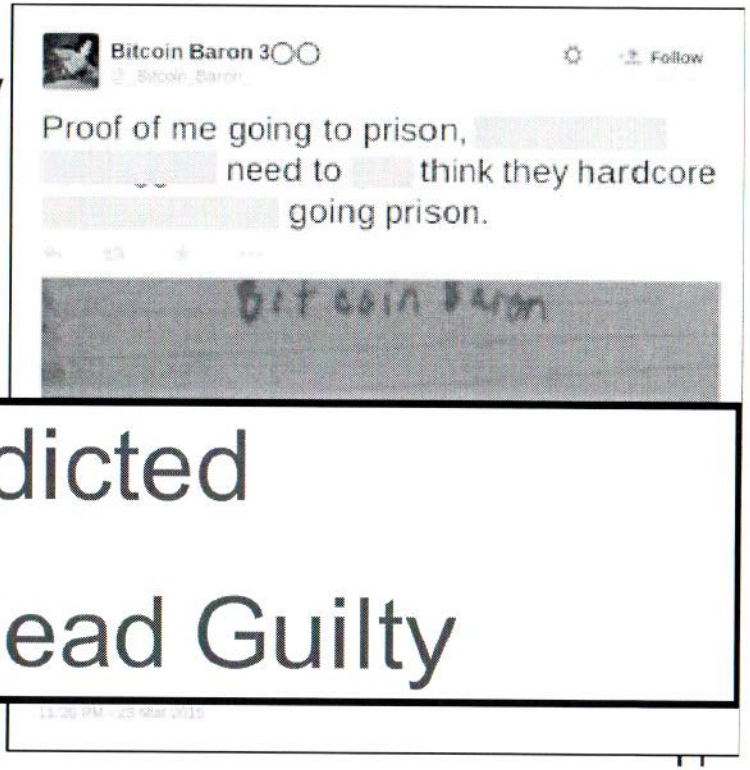


Image from Money.CNN.com

Bitcoin Baron

- December 2014 - January 2015 claimed responsibility for 11 DDoS attacks against SLTTs
- March 2015 – claimed responsibility for 11 DDoS attacks against SLTTs
- March 23, 2015 – accidentally posts an unrelated charge sheet on Twitter; pulls it offline almost immediately;



Sept 2016 – Indicted

April 17th, 2017 – Plead Guilty

Social Engineering

How well do you know me? How well do I know you??? You have 10 minutes to answer these questions and share or you will have horrible luck for 3 years!!!

2. WHEN WAS THE LAST TIME YOU CRIED? I don't remember.

...

4. WHAT IS YOUR MOM'S FULL NAME? Jane Lee Smith Wright

...

8. WHAT IS YOUR FAVORITE ICE CREAM? Strawberry

...

17. WHERE DID YOU GO TO HIGH SCHOOL? Albany High School

...

18. WHAT WAS YOUR HIGH SCHOOL MASCOT? Falcons

...

28. EYE COLOR? Brown.

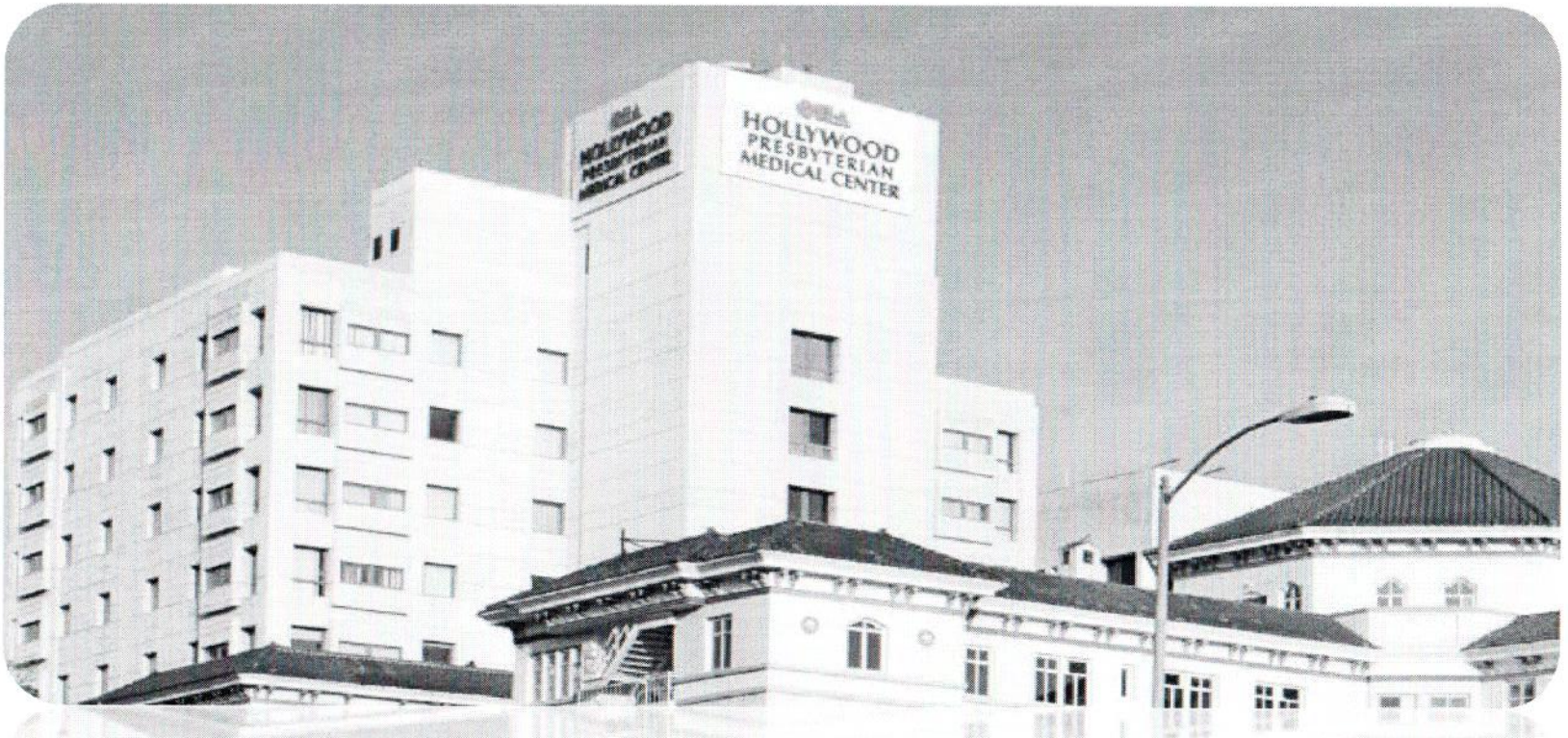
...

31. WHAT COLOR IS YOUR CAR? White

...

44. WHERE WERE YOU BORN? Albany, NY

Hollywood Presbyterian Hospital



"The quickest and most efficient way to restore our system and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this."

Los Angeles Valley College

Los Angeles Valley College had servers compromised by Ransomware
LAVC Network, email, and phone systems were brought down

$28,000 in BTC was paid to restore service

A claim has been opened with their cybersecurity insurance provider

City of Atlanta - 2018

ATLANTA SPENT $2.6M TO RECOVER FROM A $52,000 RANSOMWARE SCARE

Ransomware - Don't Be Next

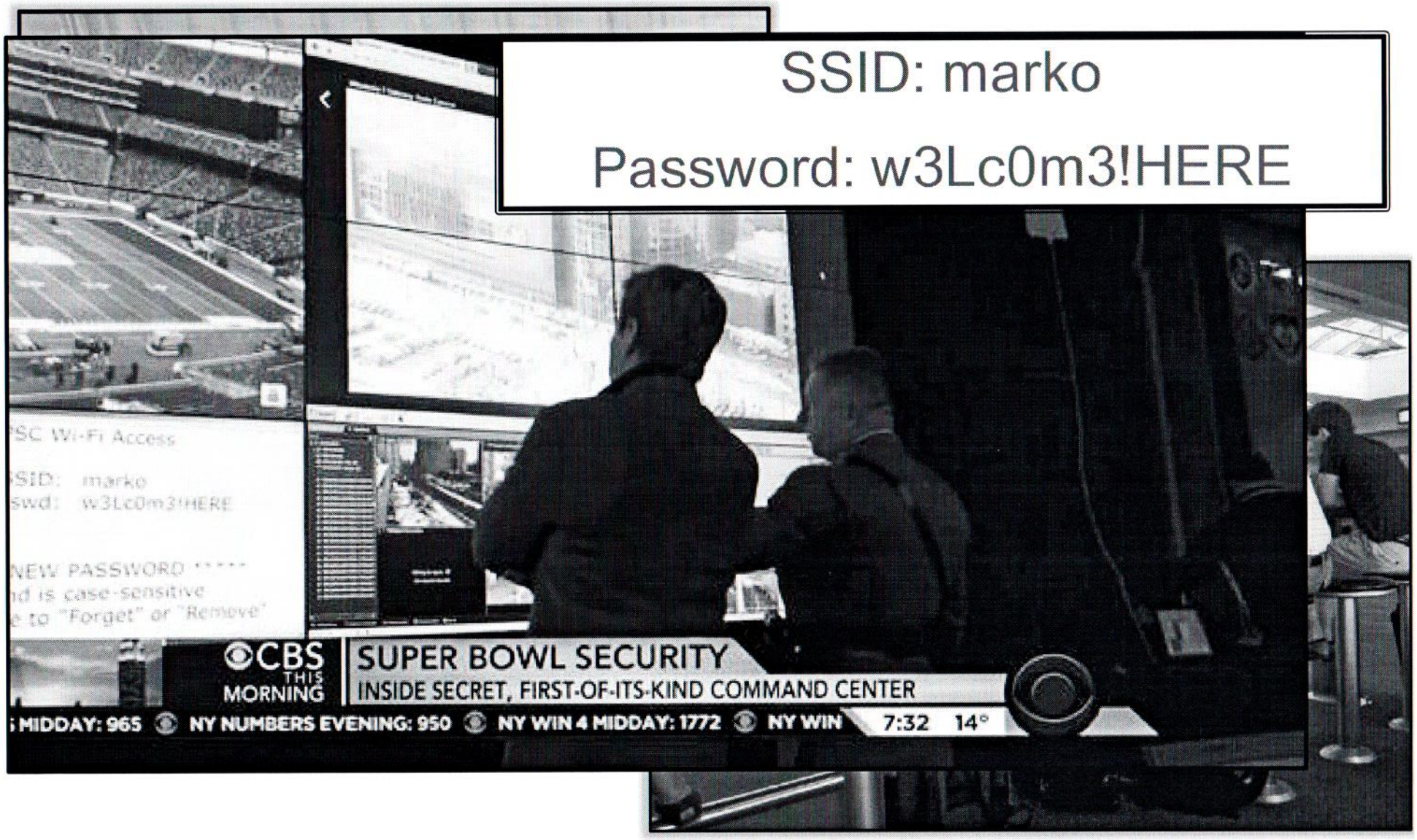
Contingency Plan

- Discuss what a ransomware infection would cost your specific agency and make decisions before infection occurs
- Keep in mind – in 15% of cases, decryption keys do not work
- Prepare and test protocols for multiple scenarios and have recovery plans in place

Prevention

- Keep your systems patched – desktops and servers
- Ensure up-to-date backups are stored offline and regularly tested
- Email filtering
- Keep your AV and firewall patched
- End user training and awareness

Employee Mistakes – Insider Threat



2 Computers in the Prison Ceiling - 2015

- Used parts from a computer recycling program
- Detected July 3, 2015, when contractor's Internet threshold was exceeded
  - Previously tried to access file-sharing sites
  - Looked for ways around the proxies
- Network cable led to the ceiling
- Forensic analysis of the hard drives found pornography, articles about making drugs, explosives and credit card fraud

The two computers were hidden on plywood boards in the ceiling

Great Falls Montana

- What happened in Great Falls?
- Emergency Alert System Hacked?
- Not quite. Rather, it took a couple of industrious/mischievous European youths simply calling up the City Department in question and politely requesting the information they needed while impersonating the vendor who supplied the equipment.

Share Information

- **Be prepared**
  - Learn from others' best practices
  - Gather intel to help you be proactive
- **Be willing to ask for help**
  - Identify other resources to augment what you are doing
- **Be a part of the solution**
  - Take part in information sharing

What can you do?

- ✓Patch!
- ✓Training
- ✓Backups
- ✓Harden Systems
- ✓Update Policies
- ✓Compliance
- ✓Scan Systems
- ✓Encrypt Mobile Devices

Computer Emergency Response Team

- Incident Response (includes on-site assistance)
- Access to CERT CIS ESP tool
- Network & Web Application Vulnerability Assessments
- Malware Analysis
- Computer & Network Forensics
- Log Analysis
- Statistical Data Analysis
- Penetration Testing

To report an incident or request assistance:
Phone: 1-866-787-4722
Email: soc@msisac.org

Monitoring of IP Range & Domain Space

IP Monitoring

- IPs connecting to malicious C&Cs
- Compromised IPs
- Indicators of compromise from the MS-ISAC network monitoring (Albert)
- Notifications from Spamhaus

Domain Monitoring

- Notifications on compromised user credentials, open source and third party information
- Vulnerability Management Program (VMP)

Send domains, IP ranges, and contact info to:
soc@msisac.org

Malicious Code Analysis Platform

A web based service that enables members to submit and analyze suspicious files in a controlled and non-public fashion

- Executables
- DLLs
- Documents
- URLs
- Quarantine files
- Archives

To gain an account contact:
mcap@cisecurity.org

Weekly Malware IPs and Domains

Automated Threat Indicator Sharing via Anomali

TLP: GREEN

ESS	LOG COUNT	EVENT COUNT	COUNTRY	ASSOCIATED THREAT
69.162	1522	5	United States	Luminosity, LuminosityLink
.108.148	969	3	United States	Luminosity
14.67	143	15	Netherlands	Generic Trojan
112.248	83	4	United States	Fleercivet
18.141	23	3	Germany	Ursnif
80.128	13	7	United States	Various malware, WS/JS Downloader
44.145	10	3	United States	Various malware, WS/JS Downloader
44.165	10	3	United States	Various malware, WS/JS Downloader
.125.32	7	4	United States	Kovter
149.172	4	4	United States	Cerber

TLP: GREEN

From: MS-ISAC SOC
To: MS-ISAC SOC
Cc:
Subject: Message from the MS-ISAC: Malware IPs and Domains observed by MS-ISAC 11/23/2

Message | IPs of Interest 11-23 to 11-29.xlsx (35 KB)

Attached to this email is a list of IP addresses and domains associated with malw

Recipients may only share TLP: GREEN information with peers and partner organizations within their sector or comm

This list is produced from data collected by the MS-ISAC. Currently this data is being collected across a number of States and Local

The spreadsheet contains four tabs with the following information:

1. Malware IP Data

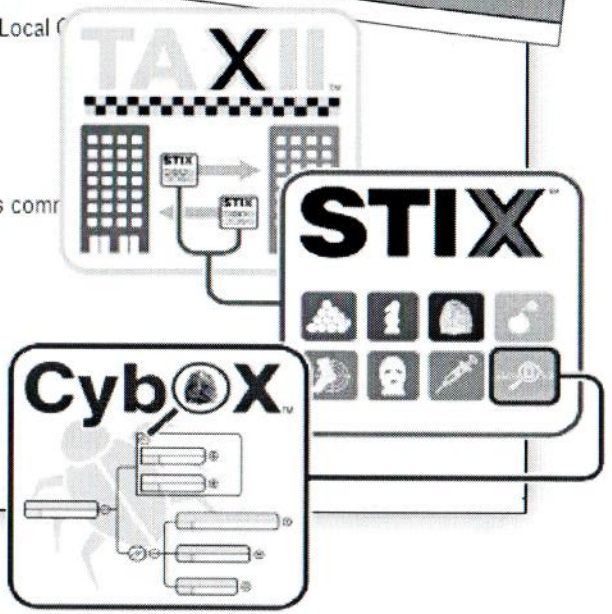
IP Address – This is either the IP address that is attacking a system or the IP address malware on an infected system is comm

Counts – This is the number of alerts generated for malicious traffic to or from the IP address.

Country, Region, City – Location of the potentially malicious IP address.

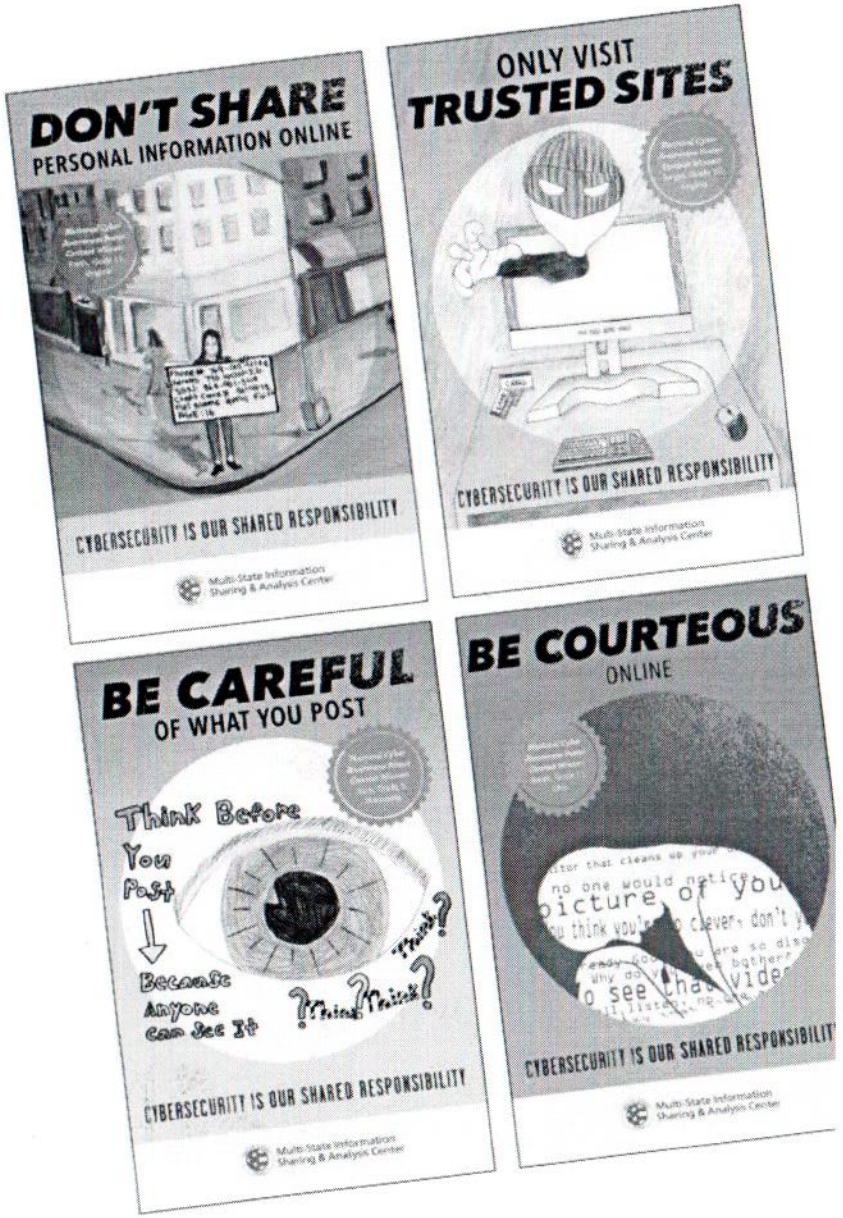
To gain an Anomali account contact:

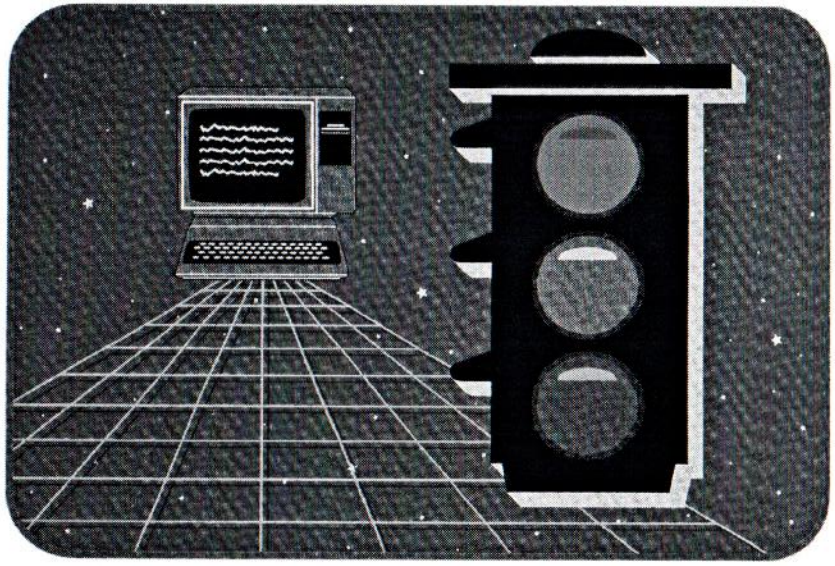
SOC@msisac.org



TLP: WHITE

Cybersecurity Awareness Toolkit





Have you logged off your terminal?

Monthly Newsletter

Distributed in template form to allow for re-branding and redistribution by <u>your</u> agency

March, 2017
Volume 12, Issue 3

Common IT Wisdom That Keeps You Secure

MS-ISAC
Multi-State Information Sharing & Analysis Center

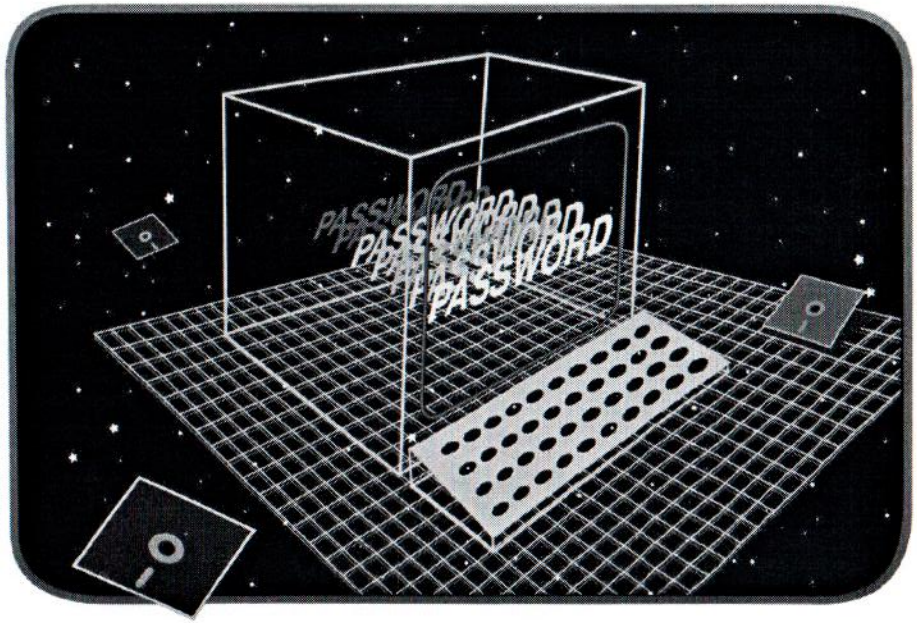
Insert your agency name and contact info here

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

Day in and day out, employees hear the same things from their IT staff about cybersecurity and safety. Though they may sound like a broken record, there are very important reasons and rationale behind these practices and advice. Keeping safe and secure while connected isn't just about how your system is set up - it is also very much about how you end up using it. Below, we discuss some common IT staff wisdom and provide some background information and the rationale as to why it definitely merits your attention.

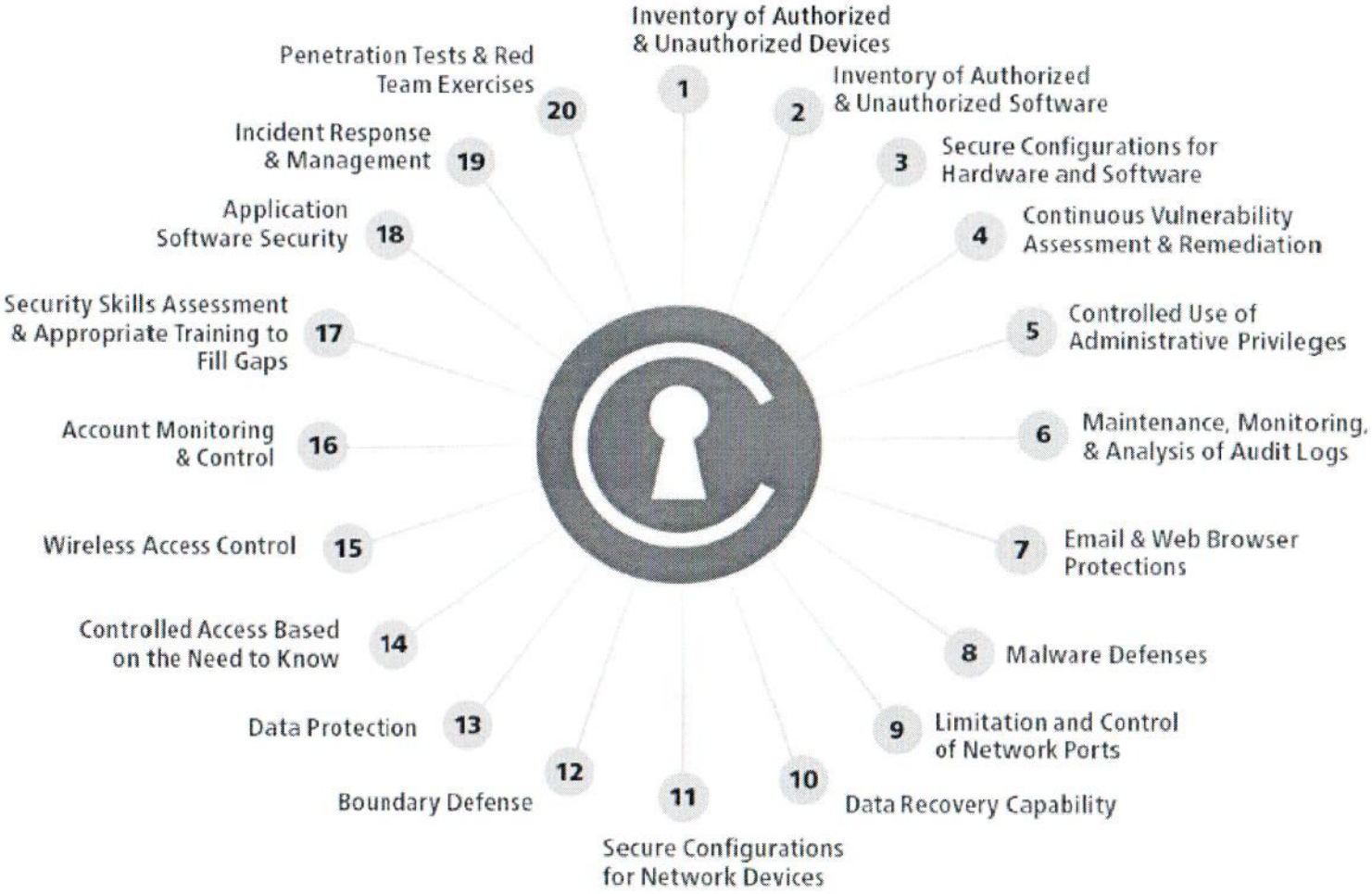
Make sure you lock your screen when you are away from your desk.

Screen locking policies exist for a reason. Even if you are leaving for just a few minutes at a time, be sure to lock your screen. Though physical intruders are rare during daytime and in conventionally secured offices, intrusions do occasionally happen. Screen locks also thwart opportunistic insider attacks from other employees that may seek to obtain information or access information beyond what they should normally have. If you don't adhere to a screen locking policy, an attacker can simply walk up and start manipulating or stealing your



"Open Sesame" isn't the secret word.
Your password is — protect it.

CIS Controls



Who do I call?

Security Operations Center (SOC)

SOC@cisecurity.org - 1-866-787-4722

31 Tech Valley Dr., East Greenbush, NY 12061-4134

www.cisecurity.org

to join or get more information:

https://learn.cisecurity.org/ms-isac-registration

CIS Center for Internet Security®

MS-ISAC
Multi-State Information Sharing & Analysis Center

MS-ISAC 24x7 Security Operations Center

1-866-787-4722

SOC@cisecurity.org

Andrew Dolan
Director of Stakeholder Engagement
MS-ISAC
Andrew.Dolan@cisecurity.org
518-880-0699

Cybersecurity Best Practices

Gerry Cochran, IT Specialist III

NYS COMPTROLLER
THOMAS P. DiNAPOLI

Agenda

- Cybersecurity Threats
- Recent Cyberattacks
- Cybersecurity best practices

Cybersecurity Threats (Network)

- Malware
- Social Engineering
- Ransomware
- Denial-of-Service (DoS) Attacks
- Man-in-the-Middle (MITM) Attacks
- Password Attacks
- Wireless Attacks
- Insider Threats

Recent Cyberattacks

The 2018 Verizon Breach Report

What tactics are being utilized?

- 48% of breaches featured hacking.
  - 56% of hacking-related breaches leveraged stolen and/or weak passwords.
- 30% included malware.
  - 49% of malware was installed via malicious email.
- 17% were social engineering attacks.
  - 76% of social engineering attacks involved phishing.
- 12% involved privilege misuse.

The 2018 Verizon Breach Report

Other noteworthy items:

- 14% of breaches involved public sector entities.
- 58% of all victims are categorized as small business.
- 76% of breaches were financially motivated.
- 68% of breaches took months or longer to discover.
- Organized crime accounts for 62% of external breaches.
- 69% of all compromised data consisted of personal and/or payment data.

Atlanta Ransomware Incident

- Impacted five of the city's 13 local government departments.
- Spent $2.6M to recover from a $52,000 ransom.
- Also delayed the budget proposal as the cyber incident compromised the budget planning system.
- This ransomware variant infiltrates by exploiting vulnerabilities or guessing weak passwords in a target's public-facing systems.
- Atlanta is still recovering from the ransomware attack.

Ygnacio Valley High School Phishing Attack

- A student used a phishing scam to access the school district's computer system and change a number of students' grades.
- The student created a fake website that looked identical to the school's and then sent emails to teachers in an attempt to get them to sign into his fake site.
- Police tracked his IP address back to his home where electronics-sniffing dogs found a flash drive hidden in a tissue box.
- The student has been arrested and charged with 14 felony counts.

Hyatt Point-Of-Sale Breach

- Impacted 41 of the company's properties worldwide.
- In several public cases, adversaries called the front desk complaining of an issue and then sent an email with supporting information.
- The email contained VBScript or Macros that downloaded malware on the computer and then stole passwords and enabled Remote Desktop.

Uber

- Exposed 57 million client records (names, email addresses, phone numbers) and 600,000 driver records (names and driver's license numbers).
- Two hackers accessed Uber's Amazon cloud account (where stored data was unencrypted).
- Uber paid $100,000 to delete the data and keep the breach quiet.

Equifax

- Exposed 145.5 million Americans' names, Social Security numbers, dates of birth and addresses. Also exposed 209,000 credit card numbers.
- Attackers exploited a vulnerability in an Equifax web application.
- Evidence of a second breach was discovered just one month later - Equifax took down a consumer webpage to investigate the possible breach.

Cybersecurity Best Practices

Hardware, Software and Data Inventories

Best Practice: Maintain detailed, up-to-date inventory records for all computer hardware, software and electronic data.

Without the proper identification of all devices on a network, unauthorized devices and software can be easily introduced, putting the network and data at risk. A single compromised device can become a launching point for further network attacks, quickly turning one compromised device into many.

Inadequate inventory records makes it unlikely that software patches necessary to address known security vulnerabilities can be applied on a timely basis, if at all.

Hardware, Software and Data Inventories (Continued)

Inadequate records increases the likelihood that you may inadvertently violate copyright laws by having more software users than licenses for a particular application and incur penalties as a result.

IT security alerts and bulletins issued by software vendors, municipal associations, and federal and state agencies reference specific types and versions of devices and software. These alerts are intended to raise awareness about threats, sometimes imminent threats, to computer systems. Accurate inventory records can help you determine if these advisories are relevant to your unique computing environment.

It is very challenging to protect computer resources, including data, if you do not know exactly what resources you have and where those resources reside.

Data Classification

Data classification is the process of assigning data to a category (e.g., public, internal use, confidential) that will determine the level of internal controls over that data.

An inventory of information assets (i.e., data) that classifies data according to its sensitivity and identifies where the data resides (e.g., servers, workstations, and laptops) is important because different kinds of information require different levels of protection.

Policies and Training

Best Practice: Adopt IT policies that define appropriate user behavior, describe the tools and procedures needed to protect data and information systems, and explain the consequences of policy violations. Provide entity-wide, cybersecurity training that is closely tied to the IT policies.

- Acceptable Use
- Breach Notification (New York State Technology Law Section 208 (8))
- Password
- Online Banking

While your IT policies tell users what to do, training provides them with the skills to do it.

Access Controls

Best Practice: Know all points of entry to your computing environment and data, and ensure that all access is authorized and secure. Use available electronic means to enforce and monitor compliance with access controls. Place particular emphasis on limiting access to and protecting personal, private, and sensitive information.

- Have written procedures in place for granting, changing, and terminating access rights.
- Allow users to access only what is necessary to complete their job duties (principle of least privilege).
- Periodically review all accounts and disable any account that cannot be associated with an authorized user.

User Accounts and Passwords

- To ensure individual accountability within the network, each user should have his or her own network account (username and password). Likewise, to ensure individual accountability within software applications, each user should have his or her own user account (username and password).
- Users should be able to set their own passwords.
- Criteria you should consider with regard to passwords:
  - Complexity requirements
  - Length
  - Aging
  - Reuse of old passwords
  - Failed log-on attempts.

Strictly Control the Use of Administrative Privileges

Administrative privileges are highly privileged accounts that generally allow users to: view all data on the system or network; make changes to the settings configured on the system or network; and create new user accounts, or change the levels of privileges granted to existing user accounts, on the system or network.

Administrative privileges are necessary for only a *small number* of users with particular job duties.

There are countless ways that attackers who gain administrative privileges can leverage their positions to increase the level of damage caused when a system or network is breached.

Antivirus Protection

Best Practice: Install antivirus software and configure it to update automatically. Force scans of all newly discovered devices, such as flash drives and digital cameras, and disable the auto-play feature for USB devices.

Antivirus software scans your computer or device and looks for certain characteristics of known malware (signatures) or other suspicious activity. If something of concern is identified, the software attempts to prevent the agent from causing harm by, for example, removing malware from within a file or quarantining files.

Since malware is constantly taking new forms, an antivirus program cannot be expected to identify and neutralize all types of malware. This is one of the reasons why multiple layers of IT security (defense in depth) are required to keep computer systems and data safe.

Patch Management

Best Practice: Adopt patch-management policies and procedures that ensure that all patches and updates are applied on a regular basis.

A "patch" is software that is used to correct a problem, such as a security vulnerability, that exists within an application or an operating system.

When security vulnerabilities in software are discovered, the software vendor typically issues a free patch (fix) to correct the problem. The patch should be applied as soon as possible to reduce the likelihood that someone with malicious intent could successfully exploit the vulnerability.

At some point, vendors discontinue issuing patches (e.g., Microsoft Windows XP).

Online Banking

Best Practice: Entities should adopt a suite of technology-based and nontechnical controls to ensure online banking is conducted as safely as possible.

- Adopt an online banking policy and enter into bank agreements.
- Segregate duties.
- Enable alerts and other security measures available from the bank.
- Set up accounts that do not have access to and/or cannot be accessed through the Internet, and use those accounts for long-term savings.
- Provide cybersecurity training to officers and employees responsible for online banking.
- Consider using a separate (dedicated) computer for online banking transactions, one that is not used for email or Internet browsing.

Online Banking (continued)

- Type the bank's website address into the Internet browser's address bar every time.
- Do not allow the computer or web browser to save online banking login names or passwords.
- Use a wired rather than wireless network for financial transactions.
- Monitor accounts on a timely basis, at least every two or three days, for unauthorized or suspicious activity.
  - Any suspicious activity should be reported immediately. There is a limited recovery window, and a rapid response may prevent additional losses.
  - To be effective, monitoring must occur frequently even during times when many personnel may be on leave (e.g., 4th of July week; the weeks before, during and immediately after Christmas).

Wireless Networks

Best Practice: Configure your wireless network to broadcast only as far as necessary, enable the best available encryption, and require strong passwords.

- Wireless access point coverage should radiate out to the windows, but not beyond.
- Enable the most-secure encryption available (currently WPA2).
- Require a strong password for connecting to the wireless network.

Public Website Information Disclosure

Best Practice: Establish a framework for classifying data based on its level of sensitivity, review ***all*** materials ***before*** they are posted to your public website, and then periodically review the content of your public website to ensure that your internal controls over sensitive information are operating as intended.

Google search operators:

- Limit search results to those that match criteria beyond simple keywords.
- Maintain a list of websites, file types, and keywords to search on a regular basis.
- Google allows users to create searches and periodically receive email alerts of new content that matches those searches.

---

http://www.googleguide.com/advanced_operators_reference.htm

http://www.google.com/alerts

Physical and Environmental Security

Best Practices: Periodically assess physical and environmental security measures to ensure they adequately protect computer resources and the facilities or infrastructure that house or support those resources from intentional or unintentional harm, loss or impairment.

- Physical access controls restrict the entry and exit of personnel and/or equipment and media from an area.
- Locks, gates and security personnel.
- Smoke detectors, fire alarms and extinguishers, protection from water damage due to plumbing leaks or other flooding, and uninterruptible power supplies.

Physical and Environmental Security (Continued)

An organization's personnel can play an important part in physical security by being trained and encouraged to question people whom they do not recognize in restricted areas.

It is important to consider and evaluate physical security measures both during normal business hours and at other times for example, when an area or building may be unoccupied.

We have found servers:

- On a basement floor in a municipality that experienced flooding in the past.
- Next to the refrigerator in a break room.
- In an open area in a recreation center.
- In a closet used daily by staff and visitors to the facility.

Firewalls

Best Practice: Install one or more securely configured firewalls, and monitor the logs and alerts the firewall(s) generate. Update the firewall rules as necessary using a formal change management control process.

Firewalls consist of hardware and/or software that control the flow of network traffic between networks or hosts (e.g., computers) that employ differing security postures or goals.

There are several types of firewalls, each with varying capabilities, to analyze network traffic and allow or block specific instances by comparing traffic characteristics to existing policies.

IT Disaster Recovery Planning

Best Practice: Develop a formal IT disaster recovery plan that addresses the range of threats to your IT system(s), distribute the plan to all responsible parties, and ensure that it is periodically tested and updated as needed.

- The plan should focus on sustaining critical business functions during and after a disruption.
- Technology recovery strategies should consider the possible restoration of hardware, applications, data and connectivity.
- The plan should include policies and procedures to ensure that all critical information is routinely backed up so that it would be available in the event of an emergency.

Backups

Best Practice: Back up data at regular intervals; verify the data has been backed up; store the backup media in a secure, off-site location; and verify the ability to restore the data backup.

While many entities perform some type of backup procedures, far fewer periodically attempt to restore a backup to ensure the process is functioning as intended and that data would be available in the event of an emergency.

As noted in the discussion of ransomware, it is important to maintain offline copies of backups in case an attack renders online files unusable.

Information Disposal and Media Sanitization

Best Practice: Adopt written policies and procedures that outline the proper process to use in verifying that personal, private and sensitive data is entirely destroyed or removed from electronic media prior to the equipment's disposal or reuse.

Local governments can contract with third parties who specialize in information disposal and media sanitation. Prior to doing so, the entity can, among other things, review and evaluate the disposal company's information security polices, require that the company be certified by a recognized trade association or similar third party, and/or require the company to provide written certification that information was disposed of in the agreed-upon manner.

National Institute of Standards and Technology http://www.nist.gov/

Contracts for IT Support Services

Best Practice: Contracts (service level agreements or SLAs) for IT support services should be in writing, clearly state the local government's security needs and expectations, and specify the level of service to be provided by the independent contractor or vendor.

The components of an SLA vary but can include: identification of the parties to the contract; definitions of terminology; term/duration of agreement; scope/subject; limitations (what, if anything, is excluded); service level objectives and performance indicators; roles and responsibilities; nonperformance impact; pricing, billing and terms of payment; security procedures; audit procedures; reporting; reviews/updates; and approvals.

Cybersecurity Experts and Resources

Center for Internet Security's Multi-State Information Sharing & Analysis Center
https://www.cisecurity.org/ms-isac

New York State Office of Information Technology Services
http://www.its.ny.gov/incident-reporting

United States Cyber Emergency Response Team
https://www.us-cert.gov

Questions?

Gerry Cochran, gcochran@osc.ny.gov

Gmail

John Bowles <hartsvillets17@gmail.com>

Webinar Registration Confirmation

1 message

gotomeetings LGSA <customercare@gotowebinar.com> Mon, Jun 4, 2018 at 12:27 PM
Reply-To: gotomeetings@osc.state.ny.us
To: hartsvillets17@gmail.com

Dear John,

Thank you for registering for "Local Officials Providing the First Line of Defense Against Cyber Attacks".

Establishing and maintaining security over municipal computer systems is an issue of concern for many local governments as they continue to be targeted by cyber attacks. Please join us for a non-technical discussion about these threats and how local leaders can work to mitigate them. Staff from the Division of Local Government and School Accountability (Applied Technology Unit) will discuss some common cyber security threats, recent cyber-attacks, and some best practices to protect your system and sensitive information

Andrew Dolan, Director of Stakeholder Engagement for the Center for Internet Security will also join the conversation to highlight the work of his organization and share his insights about the evolving threat landscape. Most importantly, presenters will emphasize the low and no-cost resources available to local official throughout the State. You will also have an opportunity to ask questions of the experts.

Please send your questions, comments and feedback to: gotomeetings@osc.state.ny.us

How To Join The Webinar

Tue, Jun 12, 2018 10:30 AM - 11:30 AM EDT

Add to Calendar: Outlook® Calendar | Google Calendar™ | iCal®

1. Click the link to join the webinar at the specified time and date:

Join Webinar

Note: This link should not be shared with others; it is unique to you.

Before joining, be sure to check system requirements to avoid any connection issues.

2. Choose one of the following audio options:

TO USE YOUR COMPUTER'S AUDIO:
When the webinar begins, you will be connected to audio using your computer's microphone and speakers (VoIP). A headset is recommended.

Webinar ID: 134-427-059

To Cancel this Registration

Gmail

John Bowles <hartsvillets17@gmail.com>

Town of Hartsville / LogRhythm Introduction

1 message

Amanda Steinmann <amanda.steinmann@logrhythm.com> Thu, Jun 14, 2018 at 5:49 PM
To: John Bowles <hartsvillets17@gmail.com>

Hi John,

Is security information and event management (SIEM) on the radar for Town of Hartsville? If so, I'd like to find out more about your top priorities for finding the right SIEM. LogRhythm helps with advanced threat detection against ransomware, DDoS, and many other common cyberthreats.

My goal is to set up a 15-minute call with you so I can:

- Understand your current strategy for threat detection and response
- Discuss what you'd like to get out of a SIEM solution
- Review some of LogRhythm's capabilities around these priorities
- Discuss next steps (if you like what you hear)

Do you have 15 minutes tomorrow for a phone call to discuss your top cybersecurity priorities? If not, let's find some time within the next few days. Book a meeting with Amanda Steinmann.

Thank you in advance,
Amanda Steinmann | LogRhythm
Sales Development Representative
(720) 548-3037
www.LogRhythm.com
Book a meeting with me