ASMGi

Cyber Security in Higher Education

September 25, 2019

Esteemed Panel … Cyber Security in Higher Education

ASMGi

Tom DeChiaro
Vice President, CIO
Drexel University

Ken Makoid
Regional Vice President Northeast Sales
Flexential

Frank Yako
CIO, Director of Strategic Initiatives
ASMGi

MODERATOR

Steve Roesing
CEO
ASMGi

Agenda

ASMGi

- *Cyber Landscape in Higher Education*
- *Discussion Topic #1 – Strategy*
- *Discussion Topic #2 – Assessments*
- *Discussion Topic #3 – Solutions*
- *Discussion Topic #4 – Data Center*
- *Conclusion + Key Points*
- *Questions + Closing Remarks*

Cyber in Higher Education is Challenging because …

Vulnerabilities and unique challenges in higher education

Data variety: Any business must protect employees, customers and internal data. This is true for higher education as well, but institutions also house, feed and protect people. They administer financial aid, accept donations, conduct research involving people and animals and create inventions and intellectual property (IP). This results in a breadth of data types rarely seen in other kinds of organizations.

Decentralization: In corporate environments, a select few manage the majority of data. Higher education operates in a largely decentralized manner. Many people with different skill sets and needs collect, process and store the data, which heightens the challenge of protecting data.

Varied rules and regulations: The wide scope of work being carried out in educational institutions is subject to many different standards, regulations and legal requirements that make it difficult to follow a single regulatory framework.

Higher education sits at a nexus. These institutions deal with innumerable compliance requirements across disciplines. While the Family Educational Rights and Privacy Act (FERPA) is an obvious exception, most cyber and privacy laws are not designed to address higher education institutions specifically. Educational institutions are nevertheless impacted. For example, the Health Information Portability and Accountability Act (HIPAA) was designed for hospitals and healthcare providers, but any campus health center or research institute may also be subject to its privacy and security requirements. Similarly, the Gramm–Leach–Bliley (GLBA) Act was meant to regulate financial institutions, but on-campus departments collecting financial information or taking payments are legally bound to restrictions related to financial privacy and safeguards.

Funding: Most organizations struggle to secure large allocations for preventative measures like cybersecurity management. For higher education, the challenge is severely magnified. In many cases, funds are influenced by lawmakers, trustees and donors. Sometimes, regulations hinder what can be done.

Educational institutions also face more difficult decisions related to funding allocations than private sector entities. It is not a simple matter of diverting funds from a marketing campaign or even shareholder dividends. For a university, funding choices often come down to decisions about specific investments in the health and wellbeing of students. Choosing between expenditures like capital improvements or scholarships and cybersecurity initiatives will never be an easy decision to make.

Cyber in Higher Education is Challenging because …

ASMGi

Cyber threats to higher education

A United States Department of Homeland Security assessment on cybersecurity risks in academia does not mince words: “We have high confidence in our primary judgment that U.S. university and college networks face a persistent threat as targets of opportunity for unwitting hosting of malicious cyber activity and cybercrime.”

In the face of considerable cyber risk, institutions need to consider four main threat actors:

Nation states – These are countries and nation-state actors looking for IP or intelligence, from cancer research to defense information such as research on missile guidance defense systems. Their primary interests are research data and personally identifiable information (PII).

Criminal syndicates – These actors are going after data they can monetize – credit cards social security numbers and other PII.

Hacktivists – Hacktivists are not typically driven by a monetary goal. They seek to embarrass institutions or otherwise reveal information to defame institutions.

Insiders – Every institution deals with people who are employed or have a relationship with the institution. Colleges and universities are no different. Disgruntled employees or otherwise misled internal actors are always a threat for fraud, unauthorized information disclosure or other breaches.

Cyber in Higher Education is Challenging because …

Threat vectors in higher education

Educational institutions face many of the same vulnerabilities as other organizations, but they are often intensified. Following are a few of the most common threat vectors:

Phishing: The average institution must contend with phishing attacks on hundreds or thousands of employees. A successful phishing attack might hit just one percent of them. Universities have tens of thousands of students, faculty, staff and alumni. More potential victims exist due to the sheer numbers and the dispersal of data throughout an institution. Phishing also presents an additional threat for universities given their historical openness for the dissemination of knowledge. For example, names, titles and contact information for university personnel are often included in publicly available online directories and organizational charts. Imagine then, how easy it would be for an attacker to contact an accounting clerk pretending to be the clerk's supervisor that is requesting an urgent wire transfer.

Software vulnerabilities: All software has vulnerabilities. That's why patches are constantly being issued by vendors. Universities face a special challenge due to the sheer volume of systems and vendors that they have work with and support. They'll never have one software vendor for all of the software they require. Student information systems, web applications and payment systems are just a few of the software systems that bad actors seek to exploit.

Access control: Educational institutions typically have a large number of people with access to different systems. Different departments, contracts and mandates all have different cybersecurity requirements. Institutions need to plan for a variety of specific requirements around access, password control, multi-factor authentication and remote access.

Viruses, malware, ransomware: These are any attack designed to cause harm to a system or steal data. Typically, these are delivered through phishing, but not always. A bad actor could gain access to one system and then use it to send malware to many other people.

The internet of things: Any cyber-to-physical connected device falls into this category, including, for example: watches and fitness trackers, door-lock security systems, security cameras, HVAC, electrical, lights and other connected infrastructure. Systems like these don't typically have the same cyber controls built into their software as an institution's other technology systems. In other words, leaders don't always realize these systems can be exploited or used as attack vectors.

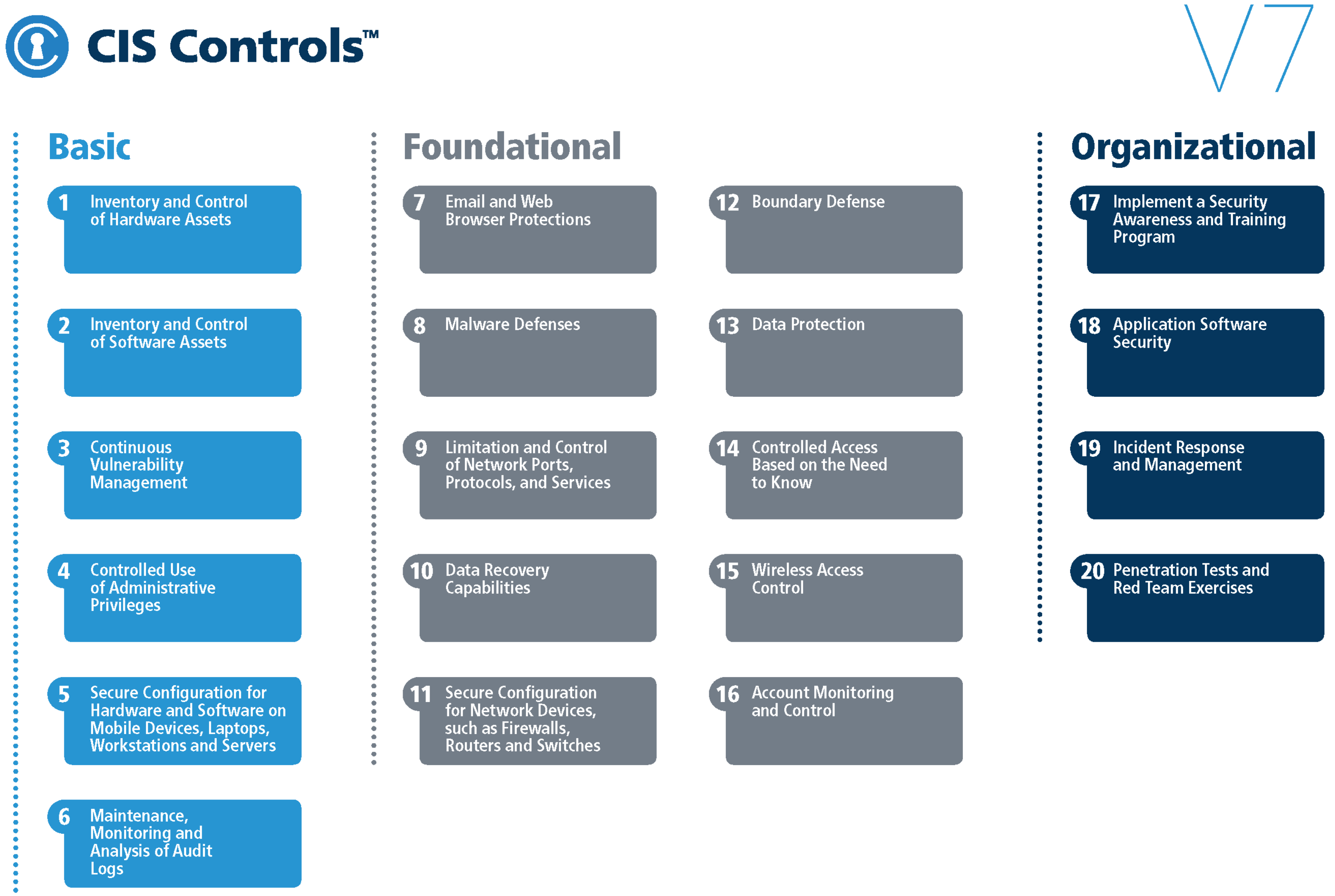
#1
STRATEGY

Does your Cyber Strategy align with your University's Strategic Plan?

How do you prioritize your initiatives?

ASMGi

Cyber Expertise prioritized Top 20



CIS Controls™ V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

How do you prioritize your initiatives?

ASMGi

Historical Breach Data annotated with CIS Controls

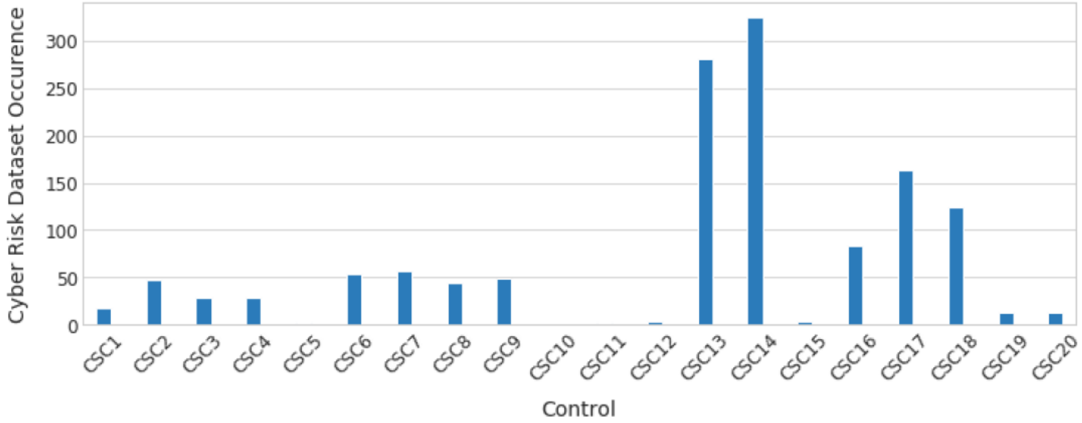
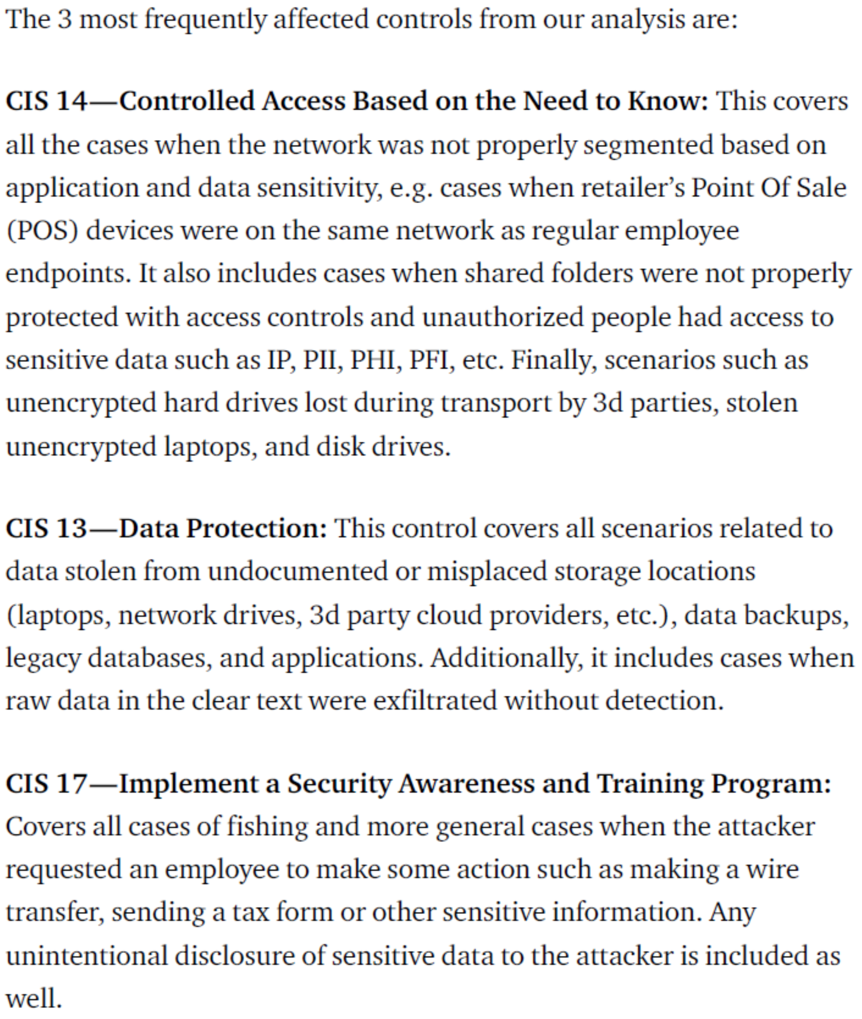


Figure 1: Shows the total number of times a CIS control could have prevented a cyber breach



The 3 most frequently affected controls from our analysis are:

CIS 14—Controlled Access Based on the Need to Know: This covers all the cases when the network was not properly segmented based on application and data sensitivity, e.g. cases when retailer's Point Of Sale (POS) devices were on the same network as regular employee endpoints. It also includes cases when shared folders were not properly protected with access controls and unauthorized people had access to sensitive data such as IP, PII, PHI, PFI, etc. Finally, scenarios such as unencrypted hard drives lost during transport by 3d parties, stolen unencrypted laptops, and disk drives.

CIS 13—Data Protection: This control covers all scenarios related to data stolen from undocumented or misplaced storage locations (laptops, network drives, 3d party cloud providers, etc.), data backups, legacy databases, and applications. Additionally, it includes cases when raw data in the clear text were exfiltrated without detection.

CIS 17—Implement a Security Awareness and Training Program: Covers all cases of fishing and more general cases when the attacker requested an employee to make some action such as making a wire transfer, sending a tax form or other sensitive information. Any unintentional disclosure of sensitive data to the attacker is included as well.

How do you prioritize your initiatives?

ASMGi

SafeBreach Attack Simulator

Gain Continuous Visibility into Your Security Posture

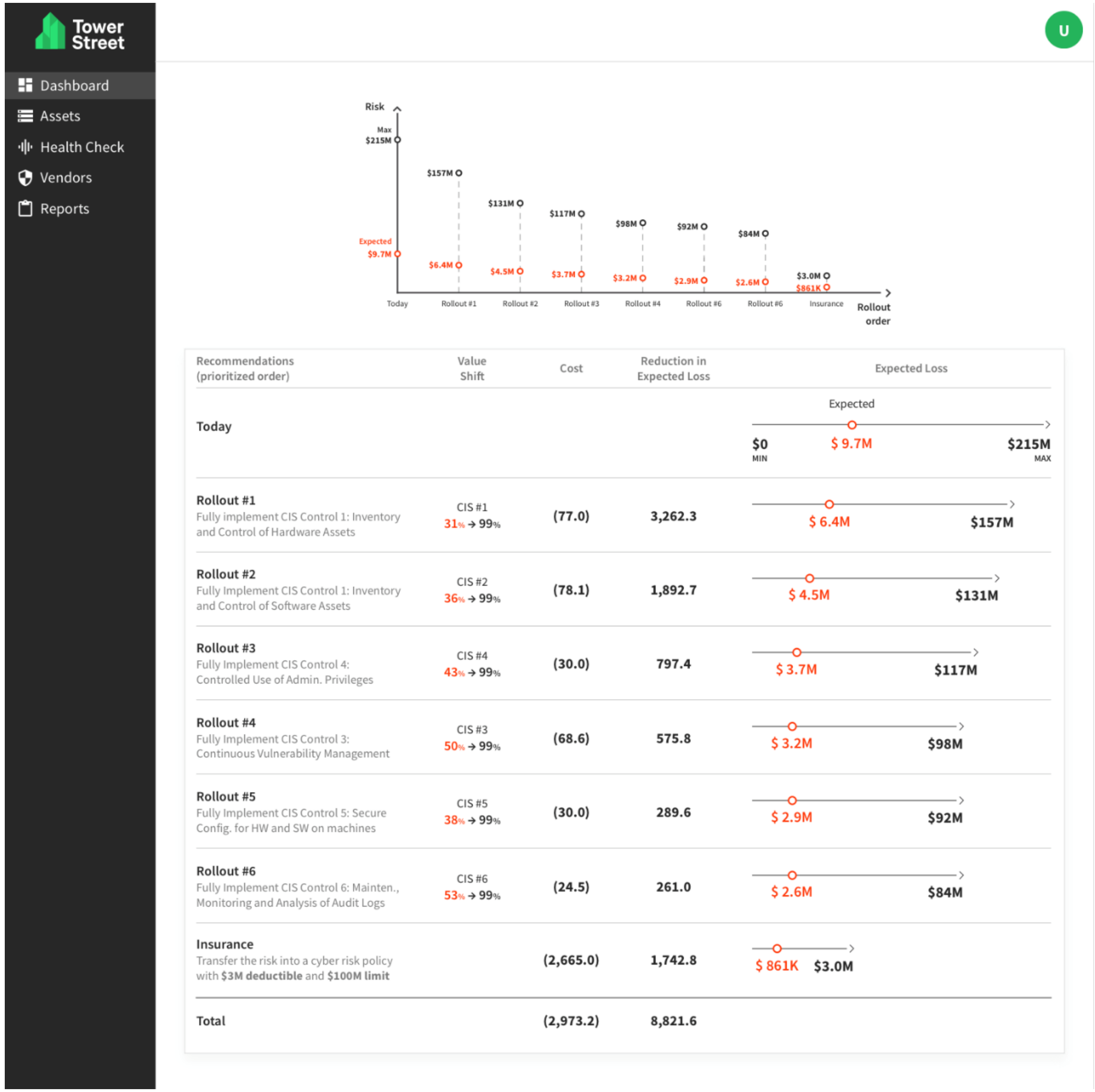
Prioritize Your Resources and Responses

Remediate Your Security Gaps

How do you prioritize your initiatives?

Quantifying Cyber Risk

- *Leverage what you have*
- *Bring security closer to the business*
- *Create a common language to discuss cyber risks*
- *Prioritization = Align budgets with initiatives that provide actual economic impact*



Recommendations (prioritized order)	Value Shift	Cost	Reduction in Expected Loss	Expected Loss
Today				Expected $0 MIN $ 9.7M $215M MAX
Rollout #1 Fully implement CIS Control 1: Inventory and Control of Hardware Assets	CIS #1 31% → 99%	(77.0)	3,262.3	$ 6.4M $157M
Rollout #2 Fully Implement CIS Control 1: Inventory and Control of Software Assets	CIS #2 36% → 99%	(78.1)	1,892.7	$ 4.5M $131M
Rollout #3 Fully Implement CIS Control 4: Controlled Use of Admin. Privileges	CIS #4 43% → 99%	(30.0)	797.4	$ 3.7M $117M
Rollout #4 Fully Implement CIS Control 3: Continuous Vulnerability Management	CIS #3 50% → 99%	(68.6)	575.8	$ 3.2M $98M
Rollout #5 Fully Implement CIS Control 5: Secure Config. for HW and SW on machines	CIS #5 38% → 99%	(30.0)	289.6	$ 2.9M $92M
Rollout #6 Fully Implement CIS Control 6: Mainten., Monitoring and Analysis of Audit Logs	CIS #6 53% → 99%	(24.5)	261.0	$ 2.6M $84M
Insurance Transfer the risk into a cyber risk policy with **$3M deductible** and **$100M limit**		(2,665.0)	1,742.8	$ 861K $3.0M
Total		(2,973.2)	8,821.6	

The Benefits of **Quantification**

ASMGi

Internal:

→ Enhances CISO and CFO / CEO dialogue and understanding

→ Financial measurement of balance sheet impact

→ Financial accuracy and substantiation of cyber budget requirements and application

→ Assimilation of cyber risk into enterprise risk management (ERM)

→ Acceptance of CISO role as a strategic function

External:

→ Enables CEO to present tangible assessment of cyber risk to stakeholders

→ Enhances financing prospects

→ Strengthening of company's position with External constituents (e.g. regulators, etc.)

→ M&A and other growth strategy advantages

→ Enables superior risk solutions (insurance; capital markets; security tech channel sales)

At the Center is CISO, CFO & CEO **Synchronicity**

#2
ASSESSMENTS

How many assessments do you do to meet your Compliance and Privacy requirements?

Compliance

PCI-DSS

HIPAA

FERPA

GLBA

FISMA

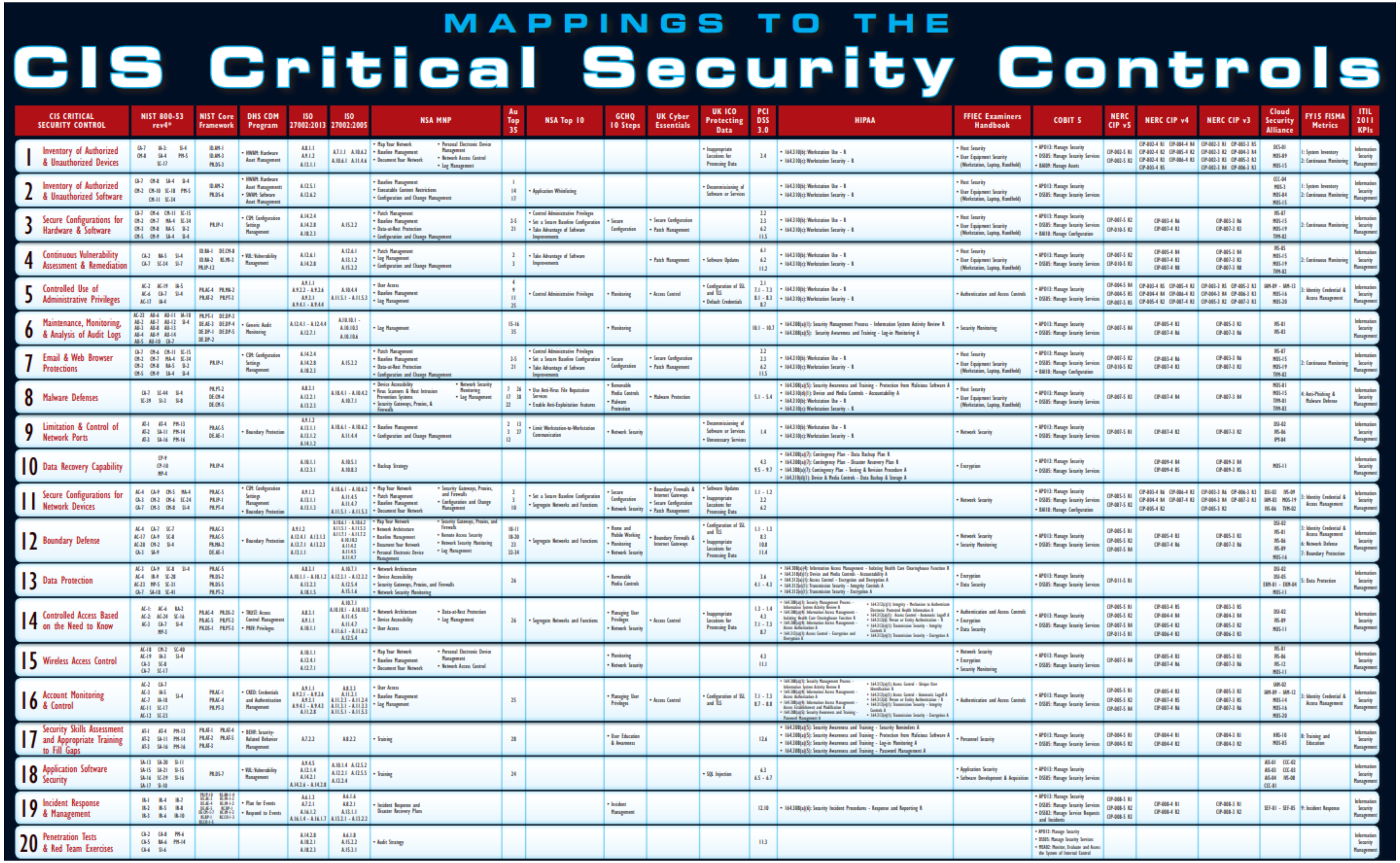
Frameworks

NIST

ISO/IEC 27001, 2

CIS

Common Controls Framework (CCF)



MAPPINGS TO THE CIS Critical Security Controls

CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
1 Inventory of Authorized & Unauthorized Devices	CA-7 IA-3 SI-4 CM-8 SA-4 PM-5 SC-17	ID.AM-1 ID.AM-3 PR.DS-3	• HWAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.1 A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI09: Manage Assets	CIP-002-5 R1 CIP-002-5 R2	CIP-002-4 R1 CIP-004-4 R4 CIP-002-4 R2 CIP-005-4 R2 CIP-002-4 R3 CIP-006-4 R3 CIP-003-4 R5	CIP-002-3 R1 CIP-003-3 R5 CIP-002-3 R2 CIP-004-3 R4 CIP-002-3 R3 CIP-005-3 R2 CIP-002-3 R4 CIP-006-3 R3	DCS-01 MOS-09 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 SA-4 SI-4 CM-2 CM-10 SC-18 PM-5 CM-11 SC-34	ID.AM-2 PR.DS-6	• HWAM: Hardware Asset Management • SWAM: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting			• Decommissioning of Software or Services		• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services				CCC-04 MOS-3 MOS-04 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
3 Secure Configurations for Hardware & Software	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	3-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R3	CIP-003-3 R6 CIP-007-3 R3	IVS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
4 Continuous Vulnerability Assessment & Remediation	CA-2 RA-5 SI-4 CA-7 SC-34 SI-7	ID.RA-1 DE.CM-8 ID.RA-2 RS.MI-3 PR.IP-12	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 3	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R2 CIP-010-5 R3	CIP-005-4 R4 CIP-007-4 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8	IVS-05 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
5 Controlled Use of Administrative Privileges	AC-2 AC-19 IA-5 AC-6 CA-7 SI-4 AC-17 IA-4	PR.AC-4 PR.MA-2 PR.AT-2 PR.PT-3		A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 25	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	2.1 7.1 - 7.3 8.1 - 8.3 8.7	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R4 CIP-004-5 R5 CIP-007-5 R5	CIP-003-4 R5 CIP-005-4 R3 CIP-004-4 R4 CIP-006-4 R3 CIP-005-4 R2 CIP-007-4 R3	CIP-003-3 R5 CIP-005-3 R3 CIP-004-3 R4 CIP-006-3 R3 CIP-005-3 R2 CIP-007-3 R3	IAM-09 - IAM-13 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
6 Maintenance, Monitoring, & Analysis of Audit Logs	AC-23 AU-6 AU-11 IA-10 AU-2 AU-7 AU-12 SI-4 AU-3 AU-8 AU-13 AU-4 AU-9 AU-14 AU-5 AU-10 CA-7	PR.PT-1 DE.DP-3 DE.AE-3 DE.DP-4 DE.DP-1 DE.DP-5 DE.DP-2	• Generic Audit Monitoring	A.12.4.1 - A.12.4.4 A.12.7.1	A.10.10.1 - A.10.10.3 A.10.10.6	• Log Management	15-16 35		• Monitoring			10.1 - 10.7	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A	• Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	IVS-01 IVS-03		Information Security Management
7 Email & Web Browser Protections	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-8 RA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	3-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R3	CIP-003-3 R6 CIP-007-3 R3	IVS-07 MOS-15 MOS-19 TVM-02	2: Continuous Monitoring	Information Security Management
8 Malware Defenses	CA-7 SC-44 SI-4 SC-39 SI-3 SI-8	PR.PT-2 DE.CM-4 DE.CM-5		A.8.3.1 A.12.2.1 A.13.2.3	A.10.4.1 - A.10.4.2 A.10.7.1	• Device Accessibility • Virus Scanners & Host Intrusion Prevention Systems • Security Gateways, Proxies, & Firewalls • Network Security Monitoring • Log Management	7 26 17 30 22	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	• Removable Media Controls • Malware Protection	• Malware Protection		5.1 - 5.4	• 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.310(d)(1): Device and Media Controls - Accountability A • 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Host Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R3	CIP-007-4 R4	CIP-007-3 R4	MOS-01 MOS-15 TVM-01 TVM-03	4: Anti-Phishing & Malware Defense	Information Security Management
9 Limitation & Control of Network Ports	AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16	PR.AC-5 DE.AE-1	• Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.2 A.14.1.2	A.10.6.1 - A.10.6.2 A.11.4.4	• Baseline Management • Configuration and Change Management	2 13 3 27 12	• Limit Workstation-to-Workstation Communication	• Network Security		• Decommissioning of Software or Services • Unnecessary Services	1.4	• 164.310(b): Workstation Use - R • 164.310(c): Workstation Security - R	• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R1	CIP-007-4 R2	CIP-007-3 R2	DSI-02 IVS-06 IPY-04		Information Security Management
10 Data Recovery Capability	CP-9 CP-10 MP-4	PR.IP-4		A.10.1.1 A.12.3.1	A.10.5.1 A.10.8.3	• Backup Strategy						4.3 9.5 - 9.7	• 164.308(a)(7): Contingency Plan - Data Backup Plan R • 164.308(a)(7): Contingency Plan - Disaster Recovery Plan R • 164.308(a)(7): Contingency Plan - Testing & Revision Procedure A • 164.310(d)(1): Device & Media Controls - Data Backup & Storage A	• Encryption	• APO13: Manage Security • DSS05: Manage Security Services		CIP-009-4 R4 CIP-009-4 R5	CIP-009-3 R4 CIP-009-3 R5	MOS-11		Information Security Management
11 Secure Configurations for Network Devices	AC-4 CA-9 CM-5 MA-4 CA-3 CM-2 CM-6 SC-24 CA-7 CM-3 CM-8 SI-4	PR.AC-5 PR.IP-1 PR.PT-4	• CSM: Configuration Settings Management • Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.3	A.10.6.1 - A.10.6.2 A.11.4.5 A.11.4.7 A.11.5.1 - A.11.5.3	• Map Your Network • Patch Management • Baseline Management • Document Your Network • Security Gateways, Proxies, and Firewalls • Configuration and Change Management	2 3 10	• Set a Secure Baseline Configuration • Segregate Networks and Functions	• Secure Configuration • Network Security	• Boundary Firewalls & Internet Gateways • Secure Configuration • Patch Management	• Software Updates • Inappropriate Locations for Processing Data	1.1 - 1.2 2.2 6.2		• Network Security	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-005-5 R1 CIP-007-5 R2	CIP-003-4 R6 CIP-006-4 R3 CIP-004-4 R4 CIP-007-4 R3 CIP-005-4 R2	CIP-003-3 R6 CIP-006-3 R3 CIP-004-3 R4 CIP-007-3 R3 CIP-005-3 R2	DSI-02 IVS-09 IAM-03 MOS-19 IVS-06 TVM-02	3: Identity Credential & Access Management	Information Security Management
12 Boundary Defense	AC-4 CA-7 SC-7 AC-17 CA-9 SC-8 AC-20 CM-2 SI-4 CA-3 SA-9	PR.AC-3 PR.AC-5 PR.MA-2 DE.AE-1	• Boundary Protection	A.9.1.2 A.12.4.1 A.13.1.3 A.12.7.1 A.13.2.3 A.13.1.1	A.10.6.1 - A.10.6.2 A.11.5.1 - A.11.5.3 A.11.7.1 - A.11.7.2 A.10.10.2 A.11.4.2 A.11.4.5 A.11.4.7	• Map Your Network • Network Architecture • Baseline Management • Document Your Network • Personal Electronic Device Management • Security Gateways, Proxies, and Firewalls • Remote Access Security • Network Security Monitoring • Log Management	10-11 18-20 23 33-34	• Segregate Networks and Functions	• Home and Mobile Working • Monitoring • Network Security	• Boundary Firewalls & Internet Gateways	• Configuration of SSL and TLS • Inappropriate Locations for Processing Data	1.1 - 1.3 8.3 10.8 11.4		• Network Security • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	DSI-02 IVS-01 IVS-06 IVS-09 MOS-16	3: Identity Credential & Access Management 6: Network Defense 7: Boundary Protection	Information Security Management
13 Data Protection	AC-3 CA-9 SC-8 SI-4 AC-4 IR-9 SC-28 AC-23 MP-5 SC-31 CA-7 SA-18 SC-41	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2		A.8.3.1 A.10.1.1 - A.10.1.2 A.13.2.3 A.18.1.5	A.10.7.1 A.12.3.1 - A.12.3.2 A.12.5.4 A.15.1.6	• Network Architecture • Device Accessibility • Security Gateways, Proxies, and Firewalls • Network Security Monitoring	26		• Removable Media Controls			3.6 4.1 - 4.3	• 164.308(a)(4): Information Access Management - Isolating Health Care Clearinghouse Function R • 164.310(d)(1): Device and Media Controls - Accountability A • 164.312(a)(1): Access Control - Encryption and Decryption A • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-011-5 R1			DSI-02 DSI-05 EKM-01 - EKM-04 MOS-11	5: Data Protection	Information Security Management
14 Controlled Access Based on the Need to Know	AC-1 AC-6 RA-2 AC-2 AC-24 SC-16 AC-3 CA-7 SI-4 MP-3	PR.AC-4 PR.DS-2 PR.AC-5 PR.PT-2 PR.DS-1 PR.PT-3	• TRUST: Access Control Management • PRIV: Privileges	A.8.3.1 A.9.1.1 A.10.1.1	A.10.7.1 A.10.10.1 - A.10.10.3 A.11.4.5 A.11.4.7 A.11.6.1 - A.11.6.2 A.12.5.4	• Network Architecture • Device Accessibility • User Access • Data-at-Rest Protection • Log Management	26	• Segregate Networks and Functions	• Managing User Privileges • Network Security	• Access Control	• Inappropriate Locations for Processing Data	1.3 - 1.4 4.3 7.1 - 7.3 8.7	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(4): Information Access Management - Isolating Health Care Clearinghouse Function R • 164.308(a)(4): Information Access Management - Access Authorization A • 164.312(a)(1): Access Control - Encryption and Decryption A • 164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A • 164.312(a)(1): Access Control - Automatic Logoff A • 164.312(d): Person or Entity Authentication - R • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Authentication and Access Controls • Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4 CIP-011-5 R1	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-006-4 R3	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-006-3 R3	DSI-02 IVS-09 MOS-11		Information Security Management
15 Wireless Access Control	AC-18 CM-2 SC-40 AC-19 IA-3 SI-4 CA-3 SC-8 CA-7 SC-17			A.10.1.1 A.12.4.1 A.12.7.1		• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control			• Monitoring • Network Security			4.3 11.1		• Network Security • Encryption • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	IVS-01 IVS-06 IVS-12 MOS-11		Information Security Management
16 Account Monitoring & Control	AC-2 CA-7 AC-3 IA-5 SI-4 AC-7 IA-10 AC-11 SC-17 AC-12 SC-23	PR.AC-1 PR.AC-4 PR.PT-3	• CRED: Credentials and Authentication Management	A.9.1.1 A.9.2.1 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.3 A.11.2.8	A.8.3.3 A.11.2.1 A.11.2.3 - A.11.2.4 A.11.3.1 - A.11.3.3 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	25		• Managing User Privileges	• Access Control	• Configuration of SSL and TLS	7.1 - 7.3 8.7 - 8.8	• 164.308(a)(1): Security Management Process - Information System Activity Review R • 164.308(a)(4): Information Access Management - Access Authorization A • 164.308(a)(4): Information Access Management - Access Establishment and Modification A • 164.308(a)(5): Security Awareness and Training - Password Management A • 164.312(a)(1): Access Control - Unique User Identification R • 164.312(a)(1): Access Control - Automatic Logoff A • 164.312(d): Person or Entity Authentication - R • 164.312(e)(1): Transmission Security - Integrity Controls A • 164.312(e)(1): Transmission Security - Encryption A	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R5 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R5 CIP-007-3 R6	IAM-02 IAM-09 - IAM-12 MOS-14 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
17 Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16	PR.AT-1 PR.AT-4 PR.AT-2 PR.AT-5 PR.AT-3	• BEHV: Security-Related Behavior Management	A.7.2.2	A.8.2.2	• Training	28		• User Education & Awareness			12.6	• 164.308(a)(5): Security Awareness and Training - Security Reminders A • 164.308(a)(5): Security Awareness and Training - Protection from Malicious Software A • 164.308(a)(5): Security Awareness and Training - Log-in Monitoring A • 164.308(a)(5): Security Awareness and Training - Password Management A	• Personnel Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R1 CIP-004-5 R2	CIP-004-4 R1 CIP-004-4 R2	CIP-004-3 R1 CIP-004-3 R2	HRS-10 MOS-05	8: Training and Education	Information Security Management
18 Application Software Security	SA-13 SA-20 SI-11 SA-15 SA-21 SI-15 SA-16 SC-39 SI-16 SA-17 SI-10	PR.DS-7	• VUL: Vulnerability Management	A.9.4.5 A.12.1.4 A.14.2.1 A.14.2.6 - A.14.2.8	A.10.1.4 A.12.5.2 A.12.2.1 A.12.5.5 A.12.2.4	• Training	24				• SQL Injection	6.3 6.5 - 6.7		• Application Security • Software Development & Acquisition	• APO13: Manage Security • DSS05: Manage Security Services				AIS-01 CCC-02 AIS-03 CCC-03 AIS-04 IVS-08 CCC-01		Information Security Management
19 Incident Response & Management	IR-1 IR-4 IR-7 IR-2 IR-5 IR-8 IR-3 IR-6 IR-10	PR.IP-10 RS.AN-1-4 DE.AE-2 RS.MI-1-2 DE.AE-4 RS.IM-1-2 DE.AE-5 RC.RP-1 DE.CM-1-7 RC.IM-1-2 RS.RP-1 RC.CO-1-3 RS.CO-1-5	• Plan for Events • Respond to Events	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	A.6.1.6 A.8.2.1 A.13.1.1 A.13.2.1 - A.13.2.2	• Incident Response and Disaster Recovery Plans			• Incident Management			12.10	• 164.308(a)(6): Security Incident Procedures - Response and Reporting R		• APO13: Manage Security • DSS05: Manage Security Services • DSS02: Manage Service Requests and Incidents	CIP-008-5 R1 CIP-008-5 R2 CIP-008-5 R3	CIP-008-4 R1 CIP-008-4 R2	CIP-008-3 R1 CIP-008-3 R2	SEF-01 - SEF-05	9: Incident Response	Information Security Management
20 Penetration Tests & Red Team Exercises	CA-2 CA-8 PM-6 CA-5 RA-6 PM-14 CA-6 SI-6			A.14.2.8 A.18.2.1 A.18.2.3	A.6.1.8 A.15.2.2 A.15.3.1	• Audit Strategy						11.3			• APO13: Manage Security • DSS05: Manage Security Services • MEA02: Monitor, Evaluate and Assess the System of Internal Control						Information Security Management

#3
SOLUTIONS

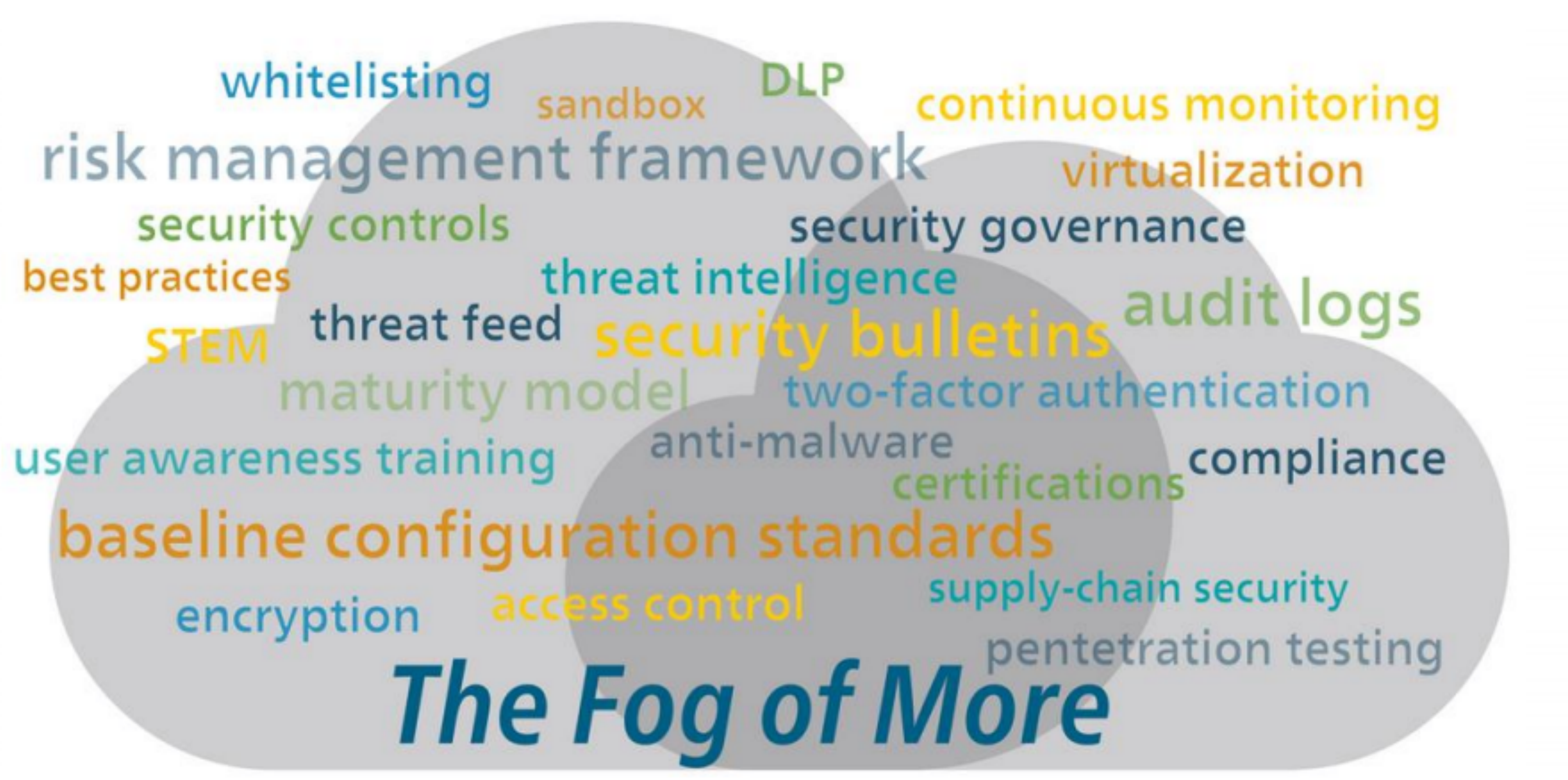
What problems are you trying to solve?

A Holistic Approach to Cyber Security

Total Solution = 3 Pillars

Program + Technology + Operations

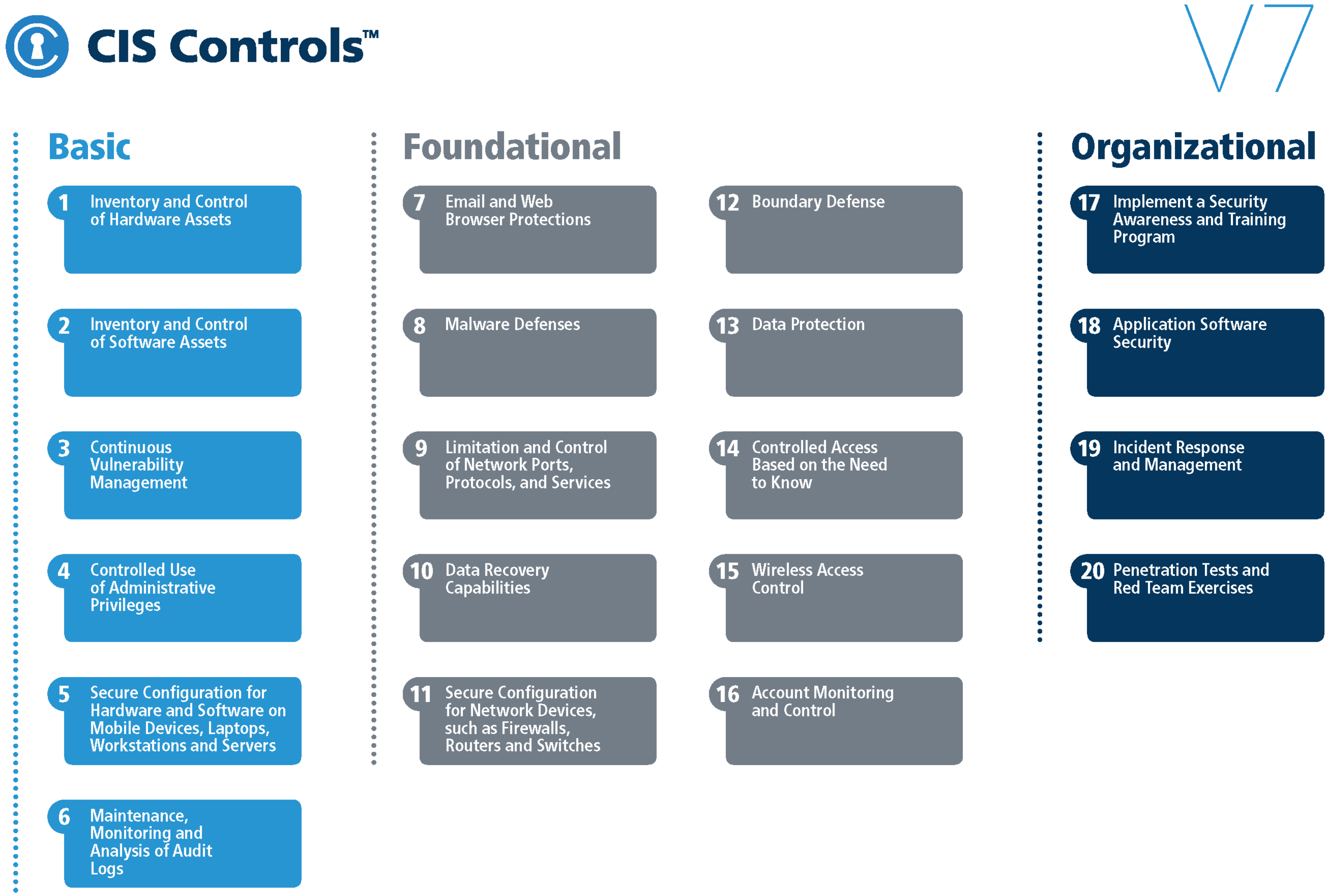
Lots to choose from …



How do you prioritize your initiatives?

ASMGi

Cyber Expertise prioritized Top 20



CIS Controls™ V7

Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

How do you prioritize your initiatives?

Historical Breach Data annotated with CIS Controls

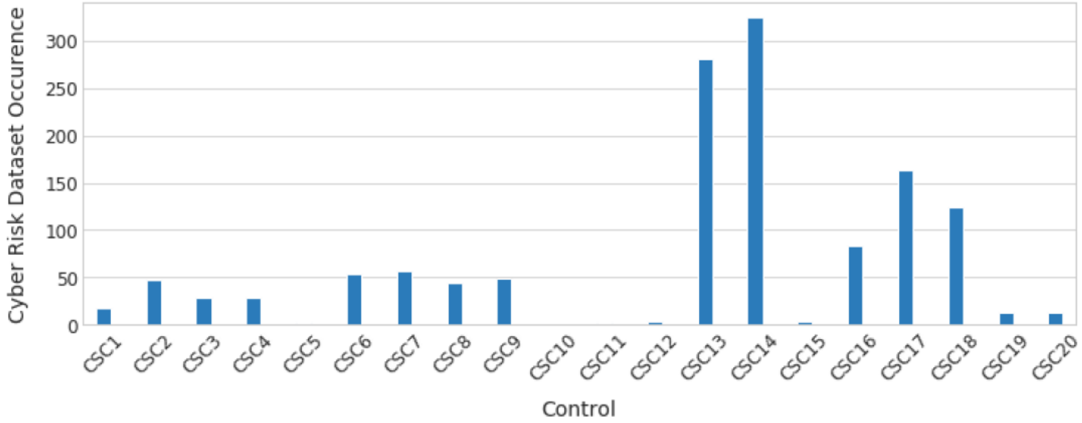
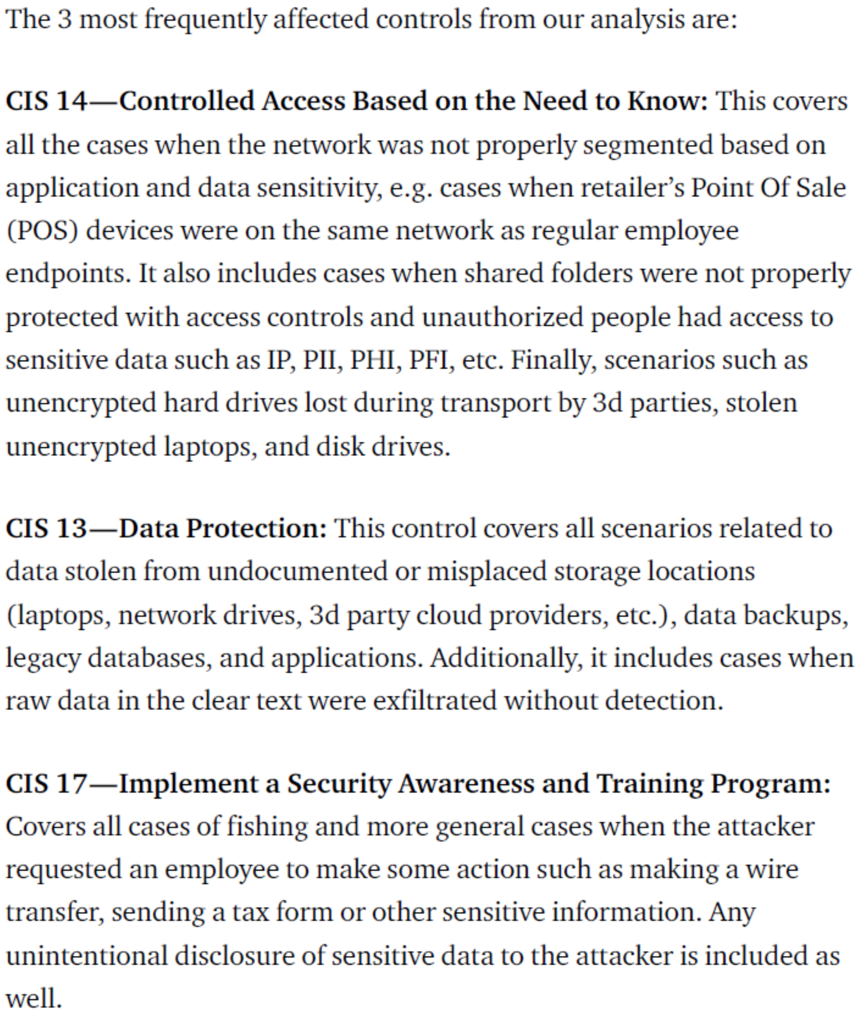


Figure 1: Shows the total number of times a CIS control could have prevented a cyber breach



The 3 most frequently affected controls from our analysis are:

CIS 14—Controlled Access Based on the Need to Know: This covers all the cases when the network was not properly segmented based on application and data sensitivity, e.g. cases when retailer's Point Of Sale (POS) devices were on the same network as regular employee endpoints. It also includes cases when shared folders were not properly protected with access controls and unauthorized people had access to sensitive data such as IP, PII, PHI, PFI, etc. Finally, scenarios such as unencrypted hard drives lost during transport by 3d parties, stolen unencrypted laptops, and disk drives.

CIS 13—Data Protection: This control covers all scenarios related to data stolen from undocumented or misplaced storage locations (laptops, network drives, 3d party cloud providers, etc.), data backups, legacy databases, and applications. Additionally, it includes cases when raw data in the clear text were exfiltrated without detection.

CIS 17—Implement a Security Awareness and Training Program: Covers all cases of fishing and more general cases when the attacker requested an employee to make some action such as making a wire transfer, sending a tax form or other sensitive information. Any unintentional disclosure of sensitive data to the attacker is included as well.

#4
DATA CENTER

Do you outsource your data center? How does your data center impact your Security?

How many of your data centers look like this?

Fully compliant solutions

Our compliance expertise runs deep with over **50** compliance-focused engineers.

ITIL®

V3 Certified

ITAR

NIST

American Institute of Certified Public Accountants Trust Services Principles for security, and availability

SOC 3 Trust Services Report

Level 1 PCI DSS service provider for colocation and cloud

ISO 27001 CERTIFIED by schellman

Information Security Management System standard

HITRUST CSF Certified

HITRUST CSF service provider for colocation and cloud

SSAE 16 CERTIFIED

SOC 1 dual-standard report

HIPAA Health Insurance Portability & Accountability Act

Health Insurance Portability and Accountability Act Security Rule

FLEXENTIAL

Colocation capability highlights

Nationwide presence and offerings for all customer types

Unique Density Footprint

- Density up to 50kw per cabinet in newer facilities

Flexible Service Options

- Inventory and terms to meet customer growth

Pricing Models To Match Customer Needs

- Fixed and variable billing options

Support points:

- 40 Datacenters
- Wholesale and Retail Colocation capability
- 100% Power SLA
- Team of Experts Available for Design, Implementation and Maintenance Needs

FLEXENTIAL

Flexential capabilities

We help organizations optimize their IT transformation journey while simultaneously balancing cost, scalability and security.

21
Domestic markets

40
Data centers

4,000
Customers

170
MW critical load UPS capacity

1,000
Employees

100Gb
Network backbone

3.1M Sq Ft
Data center footprint

31+
Industries

FLEXENTIAL

Conclusion + Key Points

ASMGi

- *Don’t recreate the wheel*
- *Map controls to complete one assessment that meets all requirements*
- *Quantify Risks to establish priority*
- *Orchestration + Automation will help meet growing demands*
- *Leverage Cyber Insurance*
- *Outsource to trusted partner when capacity or expertise is lacking*
- *There is strength in numbers! Let’s work together to help you ALL succeed!*

QUESTIONS?

Upcoming Webinars and Events

Events

- *September 25th 4PM* - ***Cyber Security Issues in Higher Education***
  panel discussion at the Union League of Philadelphia
- *October 21-25* - ***Information Security Summit***
  at The Cleveland I-X Center

Webinars

- *September 18* - ***Setting the Trap: Crafty Ways The Bad Guys Use Pretexting To Own Your Network***
  presented by KnowBe4
- *October 3* - ***Securing Your Endpoints – Why Are Businesses Getting Hit With So Much Malware?***
  presented by ASMGi and Malwarebytes
- *October 10* - ***Where Will You Compute Securely?***
  presented by ASMGi and Flexential
- *October 17* - ***Do You Know Where Your Data Is And Who Is Accessing?***
  presented by ASMGi and Heureka

ASMGi

Thank You!

800 Superior Ave E, Ste 1050
Cleveland, OH 44114

Phone: 216.255.3040
Fax: 216.274.9647

Email: info@asmgi.com

www.asmgi.com