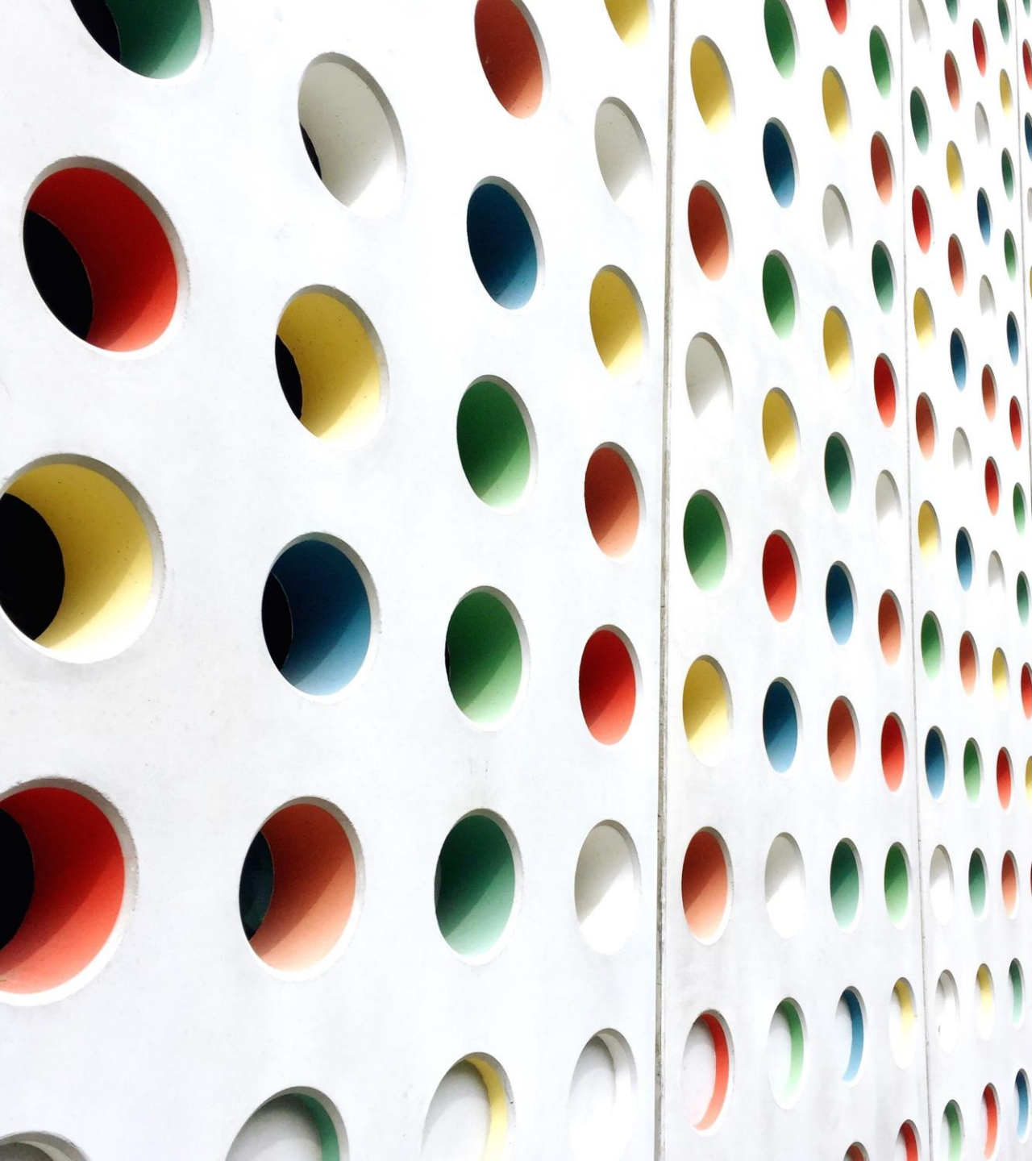


Navigating Cyber Security Insurance and Compliance

WHAT YOU NEED TO KNOW TO GET IT DONE

NETWORKS
CONSULTING RESOURCES

www.networkscr.com 888-NETWRK2

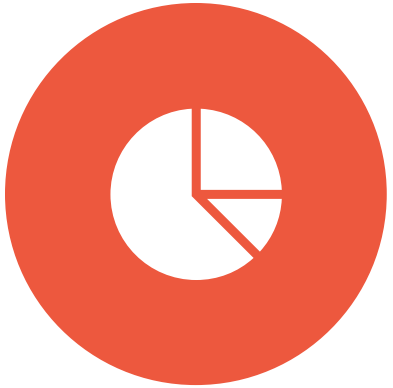
Matthew Kaseeska

Founder, CIO / CISO

- *Founded in 1997*
- *vCIO and vCISO*
- *Over 30 years in the industry*
- *MBA from MIT 2011*
    - *Focus on systems and process*

NETWORKS
CONSULTING RESOURCES

What we should focus on



USE A SYSTEM TO MEASURE YOUR EXISTING INFRASTRUCTURE.

KNOW YOUR ULTIMATE GOAL THAT YOU WANT TO ACCOMPLISH AT THE END OF THIS PROCESS.

SET A TIME FRAME, DATES AND MILESTONES TO GET IT DONE.

NETWORKS
CONSULTING RESOURCES

Top reasons companies go through compliance

Your firm or vendors require you to become compliant to their cyber security efforts

Insurance company requires your company to go through this process in order to get cyber security insurance

Your company has had an incident and needs to increase their Cyber Security Stance

CYBERSECURITY & DEFENSIBILITY

Cybersecurity is an ever-evolving landscape:

- 91% of attacks start with phishing
- 85% of attacks involve the **human** element
- **$700,000 were given to Nigerian Princes last year**
- **MFA is vulnerable to Attacker-in-the-Middle threats**
- Most business operate with multiple cloud identities to access Cloud based applications and data
- Cloud based applications and data are accessible from anywhere in the world
- Ransomware Economy – sell bits and pieces to syndicates for attacks

CYBERSECURITY & DEFENSIBILITY

Attacks are increasing in number and should be taken to be inevitable

- 83,000,000 identity attacks per Microsoft LAST MONTH
- 25.6 Billion Identity Attacks tracked by Microsoft in 2021
- FBI has identified 2000+ Ransomware attacks (reported) up to July 2022
- Estimated that 1000 Ransomware variants are created daily
- Average Cost of Breach due to Ransomware is up to $2.4 million per company
- State sponsors are creating new attacks called Zero Day attacks that security solutions have never seen before
  - **AI Runs on algorithms crafted from data (seen behaviors and events)**
  - **Need full visibility, alerting, and human evaluation to spot a zero day attack**

CYBERSECURITY & Defensibility

Cybersecurity Insurance Policies are now written to allow the insurer to **investigate and deny** claims if reasonable security measures were not fully implemented, followed, or planned on

Legislation at the State and Federal level is in progress to ensure businesses are implementing a **reasonable level of security** on their networks, within their applications, and ensuring **secured access to these applications and their data**

Ongoing **court cases** are set precedents that the FCA can be applied to businesses who have undergone a cybersecurity event in which **customer contracts have been breached** or data has been exposed as well as if an **insider tips off** when a reasonable level of cybersecurity hasn't been implemented or planned on (e.g. Rocket Jet Aerodyne Lawsuit)

- This means executives that are in charge are going to jail

CYBERSECURITY & DEFENSIBILITY

How do we ensure a robust level of **security** AND ensure ***defensibility***

- Ensure Annual Alignment with the most current CIS Controls Standard and adopt a security policy of **continuous improvement**
  - CIS has 18 controls with best practice prescriptions of various degrees to help **mitigate cybersecurity risk to businesses by over 90%**
  - Recognized as a industry standard for security
- Defensibility is proven through the implementation of an easily referenceable, valued set of best practices and documentation of implemented solutions and policy that meet those best practice requirements

CYBERSECURITY & DEFENSIBILITY

How do you ensure a robust level of security AND ensure *defensibility*

- Many are now adopting a security policy that ensures internal and external clients are well defended against the ever evolving security threats landscape. It would be wise to adopt a position to continuously strive to align with the CIS Controls Standard v8 to ensure a strong security posture.
  Our *shared* responsibility with our clients in cybersecurity is to:

  - Ensure alignment to best practices and the CIS Cybersecurity referential framework
  - Ensure customer alignment to a security posture that best fits their risk
  - Ensure alignment to Cybersecurity insurance expectations
  - Ensure legal alignment to appropriate and applicable state and federal legislation around security and privacy

NETWORKS
CONSULTING RESOURCES

CIS Security controls

Control 01 – Inventory and Control of Enterprise assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Control 02 - Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Control 03 – Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Control 04 – Secure configuration of enterprise assets and software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Control 05 – Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Control 06 – Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Control 07 – Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Control 08 – Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Control 09 – email and web browser protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Control 10 – Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Control 11 – Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Control 12 – Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Control 13 – Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Control 14 – Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Control 15 – Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Control 16 – Applications Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Control 17 – Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Control 18 – Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

NETWORKS
CONSULTING RESOURCES

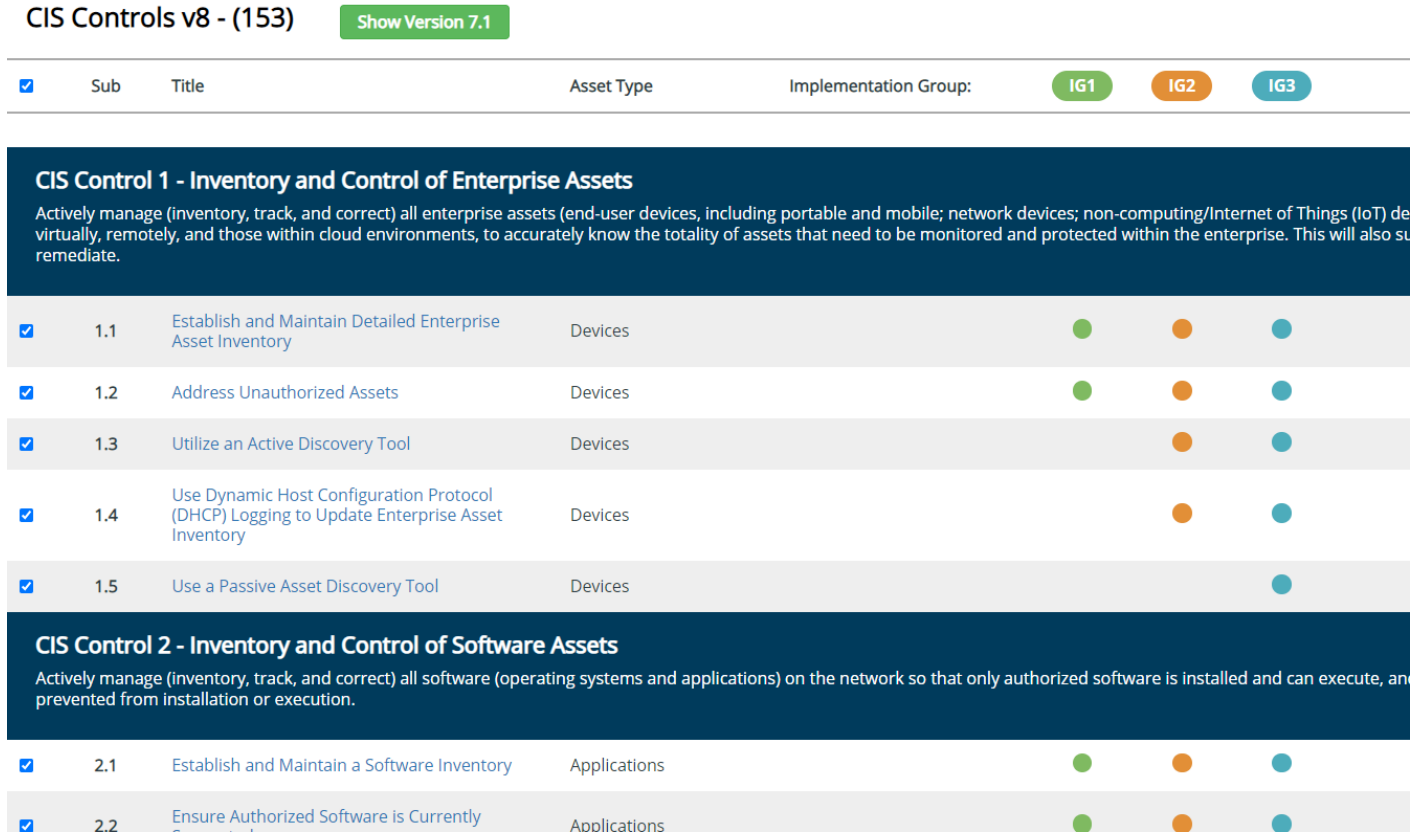
CIS Security Controls

How do you eat an Elephant?

One bite at a time:)

There are 3 implementation group levels for the 18 CIS Security Controls (IG1 / IG2 / IG3) Firms start with IG1 and it can take 6-24 months with planning, procurement and available resources. Most Firms have some of these controls in place already. Some companies outsource this if they have a heavy workload.

- Inventory and Control of Assets
- Inventory and Control of Software Assets
- Data Protection



CIS Controls v8 - (153) Show Version 7.1

Sub	Title	Asset Type	Implementation Group:	IG1	IG2	IG3
CIS Control 1 - Inventory and Control of Enterprise Assets Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) de virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also su remediate.						
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Devices		●	●	●
1.2	Address Unauthorized Assets	Devices		●	●	●
1.3	Utilize an Active Discovery Tool	Devices			●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Devices			●	●
1.5	Use a Passive Asset Discovery Tool	Devices				●
CIS Control 2 - Inventory and Control of Software Assets Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, an prevented from installation or execution.						
2.1	Establish and Maintain a Software Inventory	Applications		●	●	●
2.2	Ensure Authorized Software is Currently	Applications		●	●	●

As you can see, you have each control and then the three groups IG1, IG2, IG3

Determining what group you need to comply with will determine the amount of effort

https://www.cisecurity.org/controls/cis-controls-navigator/

Thank You, Hope this was helpful!

If you would like this slide deck email me at matt@networkscr.com or hit me up in Linked In

Matt Kaseeska – Net Works Consulting Resources