



# The MSP's Road to Compliance

April 11, 2023

# Today's Speakers



**Juan Fernandez**

Global Channel Chief, HacWare



**Dominickus Wells**

Partner Alliance Manager, DNSFilter



# Overview

- What is compliance? Why does it matter?
- Understanding the new MSP landscape
- How to leverage CIS as a sales tool
- Takeaways and Q&A

# What's the deal with compliance?

The unrelenting rise of cyber attacks year over year is an issue that is to be taken seriously by IT teams, *big or small*.

**58% of SMBs experienced a cyber attack in 2022**

**\$10.5 trillion** in global damages from cybercrime by 2025

There is mounting pressure for MSPs to adopt and implement a mature cybersecurity framework as regulations come from governments and demand from SMBs increase.

**Because of this, DNSFilter & HacWare are dedicated to helping MSPs through their compliance journey.**



**CMMC**  
**ACCREDITATION BODY**

Cybersecurity Maturity Model Certification



**Center for  
Internet Security®**





# Why does it matter?

- ✓ Reduce the risk of cyber attacks
- ✓ Compliance framework = **business opportunity for MSPs**
- ✓ Walk the walk: Show your customers that you take their security seriously
- ✓ SMBs are NOT cutting back on IT spend

# Why now?

"The federal government has defined what an MSP is in their groundbreaking Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCI). This is big news for every MSP in the market, as CIRCI may forever change how MSPs report and manage cybersecurity...

If you're an MSP and have no security program, no way to report an incident, no incident response plan, and no procedures in place, then you cannot possibly meet the requirements being laid out in CIRCI. Currently, we are in a holding period that could last until 2025 while these policies are being developed. During this time, MSPs must start establishing a cybersecurity incident response program within their organizations."

- Matt Lee

Security

# Congress Has Set New Rules for MSPs. Now What?

How regulations will affect the cybersecurity industry.

Dec 14, 2022 • By: [Matt Lee](#)

# Which frameworks are relevant for MSPs?

Framework or Regulation	Level of Use	Level of Concern
CIS	34%	26%
CMMC	30%	26%
COBIT	27%	23%
NIST	22%	19%
ISO 27001	21%	15%
NCSC (National Cyber Security Centre)	18%	20%
HIPAA	18%	13%
Zero Trust	14%	7%
ASD Essential 8	14%	13%
PCI-DSS	12%	10%
SOC II	11%	7%
MITRE ATT&CK	9%	9%
Other	5%	N/A
None	3%	27%

\*Data acquired from a recent Datto survey of 2,913 IT decision makers

# Initial assessment evolution

## Assessment Alignment:

Consistency across the program with precise connections between evaluations, goals and tasks.

Align objectives with strategies in your assessments to ensure that everyone involved is aware of the expectations.

<b>CONTROL 01</b> Inventory and Control of Enterprise Assets 5 Safeguards 101 2/5 102 4/5 103 5/5	<b>CONTROL 02</b> Inventory and Control of Software Assets 7 Safeguards 101 3/7 102 6/7 103 7/7	<b>CONTROL 03</b> Data Protection 14 Safeguards 101 6/14 102 12/14 103 14/14
<b>CONTROL 04</b> Secure Configuration of Enterprise Assets and Software 12 Safeguards 101 7/12 102 11/12 103 12/12	<b>CONTROL 05</b> Account Management 6 Safeguards 101 4/6 102 6/6 103 6/6	<b>CONTROL 06</b> Access Control Management 8 Safeguards 101 5/8 102 7/8 103 8/8
<b>CONTROL 07</b> Continuous Vulnerability Management 7 Safeguards 101 4/7 102 7/7 103 7/7	<b>CONTROL 08</b> Audit Log Management 12 Safeguards 101 3/12 102 11/12 103 12/12	<b>CONTROL 09</b> Email and Web Browser Protections 7 Safeguards 101 2/7 102 6/7 103 7/7
<b>CONTROL 10</b> Malware Defenses 7 Safeguards 101 3/7 102 7/7 103 7/7	<b>CONTROL 11</b> Data Recovery 5 Safeguards 101 4/5 102 5/5 103 5/5	<b>CONTROL 12</b> Network Infrastructure Management 8 Safeguards 101 1/8 102 7/8 103 8/8
<b>CONTROL 13</b> Network Monitoring and Defense 11 Safeguards 101 0/11 102 6/11 103 11/11	<b>CONTROL 14</b> Security Awareness and Skills Training 9 Safeguards 101 8/9 102 9/9 103 9/9	<b>CONTROL 15</b> Service Provider Management 7 Safeguards 101 1/7 102 4/7 103 7/7
<b>CONTROL 16</b> Applications Software Security 14 Safeguards 101 0/14 102 11/14 103 14/14	<b>CONTROL 17</b> Incident Response Management 9 Safeguards 101 3/9 102 8/9 103 9/9	<b>CONTROL 18</b> Penetration Testing 5 Safeguards 101 0/5 102 3/5 103 5/5



# Getting started

## CIS Critical Security Controls Version 8

The CIS Critical Security Controls (CIS Controls) are a prioritized set of Safeguards to mitigate the most prevalent cyber-attacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, Work-from-Home, and changing attacker tactics prompted the update and supports an enterprise's security as they move to both fully cloud and hybrid environments.

[Learn about CIS Controls v8](#)[Tools and Resources](#)[Policy Templates](#)[Companion Guides](#)[CIS Controls v8 Mappings](#)[CIS Controls v8 Translations](#)

# Let's talk about CIS

## Control 8: Audit Log Management

Log collection and analysis is critical for an enterprise's ability to detect malicious activity quickly. Attackers know that many enterprises keep audit logs for compliance purposes, but rarely analyze them.

Attackers use this knowledge to hide their location, malicious software, and activities on victim machines. Due to poor or nonexistent log analysis processes, attackers sometimes control victim machines for **months or years** without anyone in the target enterprise knowing.

### CONTROL 08

## Audit Log Management

SAFEGUARDS TOTAL

12

IG1

3/12

IG2

11/12

IG3

12/12

#### 8.6 Collect DNS Query Audit Logs

Network

Detect

Collect DNS query audit logs on enterprise assets, where appropriate and supported.

#### 8.7 Collect URL Request Audit Logs

Network

Detect

Collect URL request audit logs on enterprise assets, where appropriate and supported.

# Let's talk about CIS

## Control 9: Email & Web Browser Protections

### CONTROL 09 Email and Web Browser Protections

SAFEGUARDS TOTAL

7

IG1

2/7

IG2

6/7

IG3

7/7

#### 9.2 Use DNS Filtering Services

Network

Protect



Use DNS filtering services on all enterprise assets to block access to known malicious domains.

#### 9.3 Maintain and Enforce Network-Based URL Filters

Network

Protect



Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.

Web browsers are a very common point of entry for attackers because of their direct interaction with users inside an enterprise.

Content can be crafted to entice or spoof users into:

- Disclosing credentials
- Providing sensitive data
- Allowing attackers access through an open channel

All of which increase risk to the enterprise.

**Email and web = prime targets** for malicious code & social engineering as users interact with external and untrusted users and environments most via these means.

# 80%

of organizations say that awareness training reduced their employees' susceptibility against phishing attacks

# 90%

of all data breaches occur due to phishing attacks

# 65%

of phishing attacks are Spear Phishing, making it the most common phishing attack

## Let's talk about CIS

### Control 14: Security Awareness and skills training

The first step to reducing risk is education.

#### CIS 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.

✓	14.1	Establish and Maintain a Security Awareness Program	N/A	●	●	●
✓	14.2	Train Workforce Members to Recognize Social Engineering Attacks	N/A	●	●	●
✓	14.3	Train Workforce Members on Authentication Best Practices	N/A	●	●	●
✓	14.4	Train Workforce on Data Handling Best Practices	N/A	●	●	●
✓	14.5	Train Workforce Members on Causes of Unintentional Data Exposure	N/A	●	●	●
✓	14.6	Train Workforce Members on Recognizing and Reporting Security Incidents	N/A	●	●	●
✓	14.7	Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates	N/A	●	●	●
✓	14.8	Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks	N/A	●	●	●

# CMMC v1.02 Level 3 & 4

## CMMC v1.02 Level 3 – SC.3.192

SC.3.192 requires organizations to implement Domain Name System (DNS) filtering services. This requirement intends to reduce the organization's attack surface and should materially reduce the possible number of domains and networks DNS will allow.

## CMMC v1.02 Level 4 – SC.4.199

SC.4.199 requires organizations to utilize threat intelligence to block DNS requests from reaching malicious domains.





# Cyber Essentials

For UK MSPs

Cyber Essentials is an effective, UK Government backed scheme that will help protect organizations, regardless of size, against the most common cyber attacks.

There are two levels of certification:

1. Cyber Essentials (Self Attestation)
2. Cyber Essentials Plus (Hands-On Technical Verification)

As of today, nothing that states “DNS” or “Web” security specifically—only software based firewall.

MSPs can get ahead of others by adding a solid DNS filtering solution.

Downtime is now costing

**\$126,000**

on average

Only

**54%**

of SMBs are somewhat satisfied  
with their current security solutions

## Compliance: A business opportunity for MSPs

- Nearly 3 out of 4 companies say that a ransomware attack would be a death blow
- Rising cybercrime rates and growing awareness have led to increases in IT security budgets
- Shortage of security talent provides MSPs with opportunities to position as the cybersecurity experts

# Build a culture of security consciousness

1. Eliminate the cyber threat risk level
2. Increase user alertness to phishing risks
3. Instill a cybersecurity culture and create cybersecurity heroes
4. Change behavior to eliminate the automatic trust response





## The CIS Framework for Professional IT Management

### The First Ten Principles

- 1 Fully document what you have.
- 2 Fully document EVERYTHING that you do.
- 3 Continually monitor for changes and vulnerabilities.
- 4 Identify and rank all single points of failure and business risk.
- 5 Establish Standard Operating Procedures for all repeatable tasks.
- 6 Establish training and staff development plans for all IT staff.
- 7 Adopt a Continual Service Improvement model.
- 8 Implement Business Continuity and Disaster Recovery Plans.
- 9 Become a Security First organization.
- 10 Provide exceptional customer service to your staff and clients.

© 2021, CIS Technical Services Inc.



The top half of the image features several thick, vibrant blue lines that sweep across the black background in various directions, creating a sense of motion and energy.

# Questions?