The MSP's Road to Compliance

April 11, 2023

HacWare DNSFilter

Today’s Speakers

Juan Fernandez
Global Channel Chief, HacWare

HacWare

Dominickus Wells
Partner Alliance Manager, DNSFilter

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

CIS Center for Internet Security®

CYBER ESSENTIALS CERTIFIED

Information Security Management ISO 27001 Certified

HacWare DNSFilter

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

HacWare DNSFilter

Why now?

"The federal government has defined what an MSP is in their groundbreaking Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). This is big news for every MSP in the market, as CIRCIA 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 CIRCIA. 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

HacWare DNSFilter

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.

HacWare DNSFilter

Getting started

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	IG1	IG2	IG3
12	3/12	11/12	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.					

HacWare DNSFilter

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** Use DNS filtering services on all enterprise assets to block access to known malicious domains.	Network	Protect	●	●	●
9.3	**Maintain and Enforce Network-Based URL Filters** 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.	Network	Protect		●	●

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.

HacWare DNSFilter

80%

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

90%

of all data breaches occur due to phishing attacks

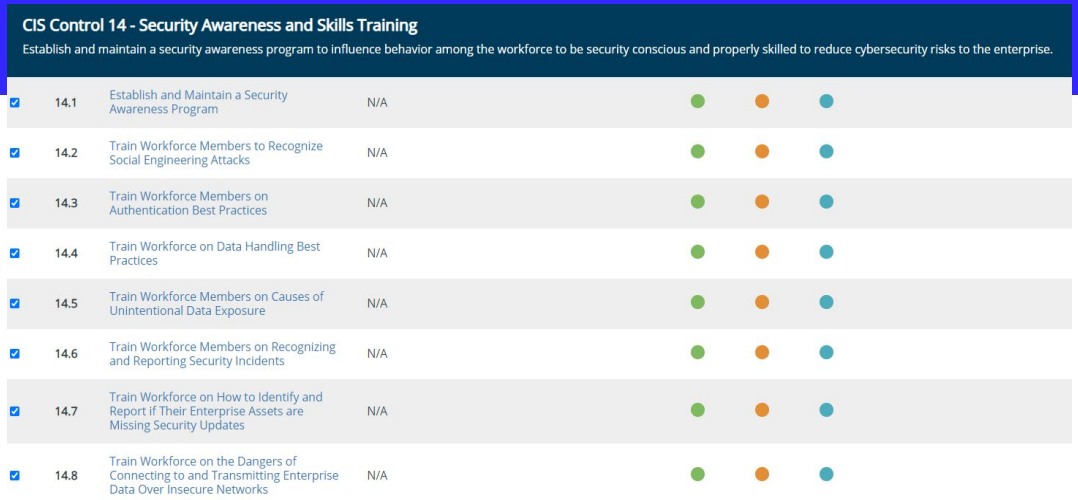
65%

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	

HacWare DNSFilter

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.

HacWare DNSFilter

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.

HacWare DNSFilter

Downtime is now costing

$126,000

on average

Only

54%

of SMBs are somewhat satisfied with their current security solutions

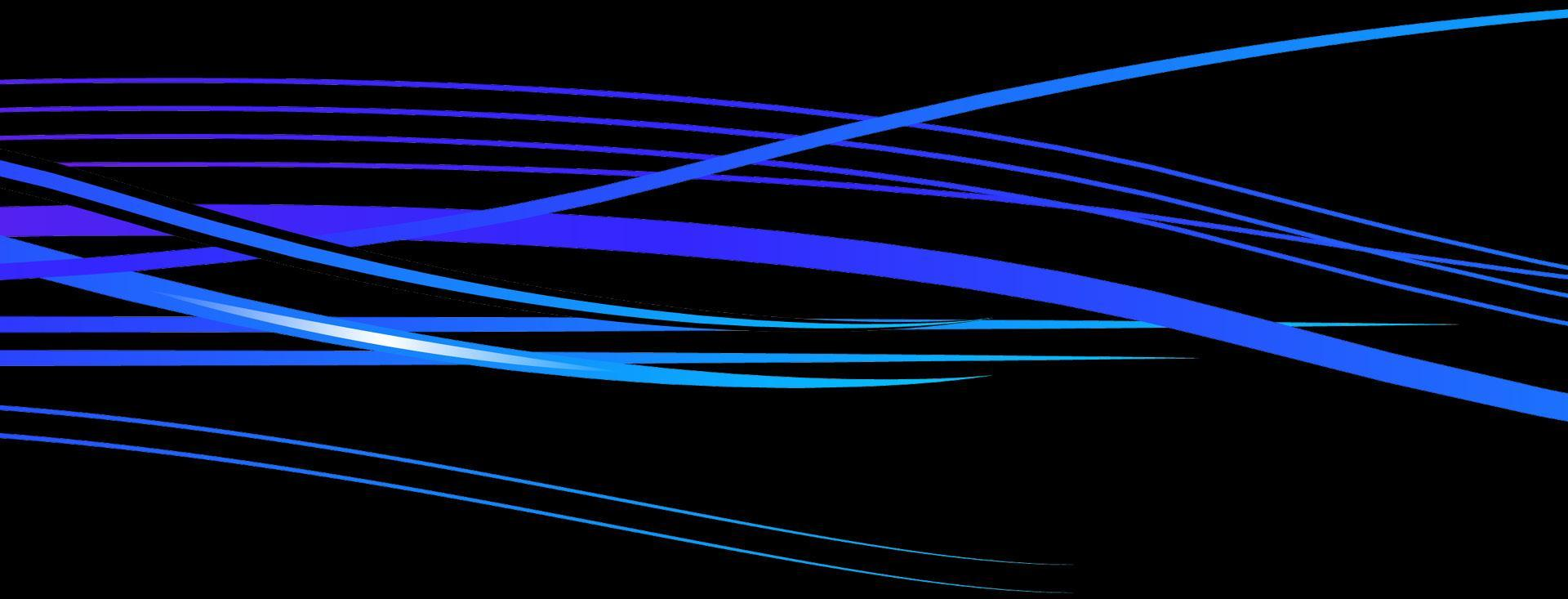
Compliance: A business opportunity for MSPs

- 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

HacWare DNSFilter



Questions?

HacWare DNSFilter