SharkStriker

GUIDE

Cybersecurity and Compliance Guide for MSPs

A detailed guide for MSPs to keep their business & customers secure and compliant.

www.sharkstriker.com

Contents

Introduction

In the last week of May, a newly emerged ransomware group, DragonForce targeted multiple organizations by initially targeting the MSP associated with them. They gained initial access by exploiting the security flaws in their remote monitoring and management tool, Simple Help.

DragonForce emerged as a new nightmare for organizations in April when a cybercrime cartel called Spider used its ransomware to infect major retailers in the UK and the US. It also offers a service that provides the infrastructure to cybercriminals to create and deploy any kind of ransomware.

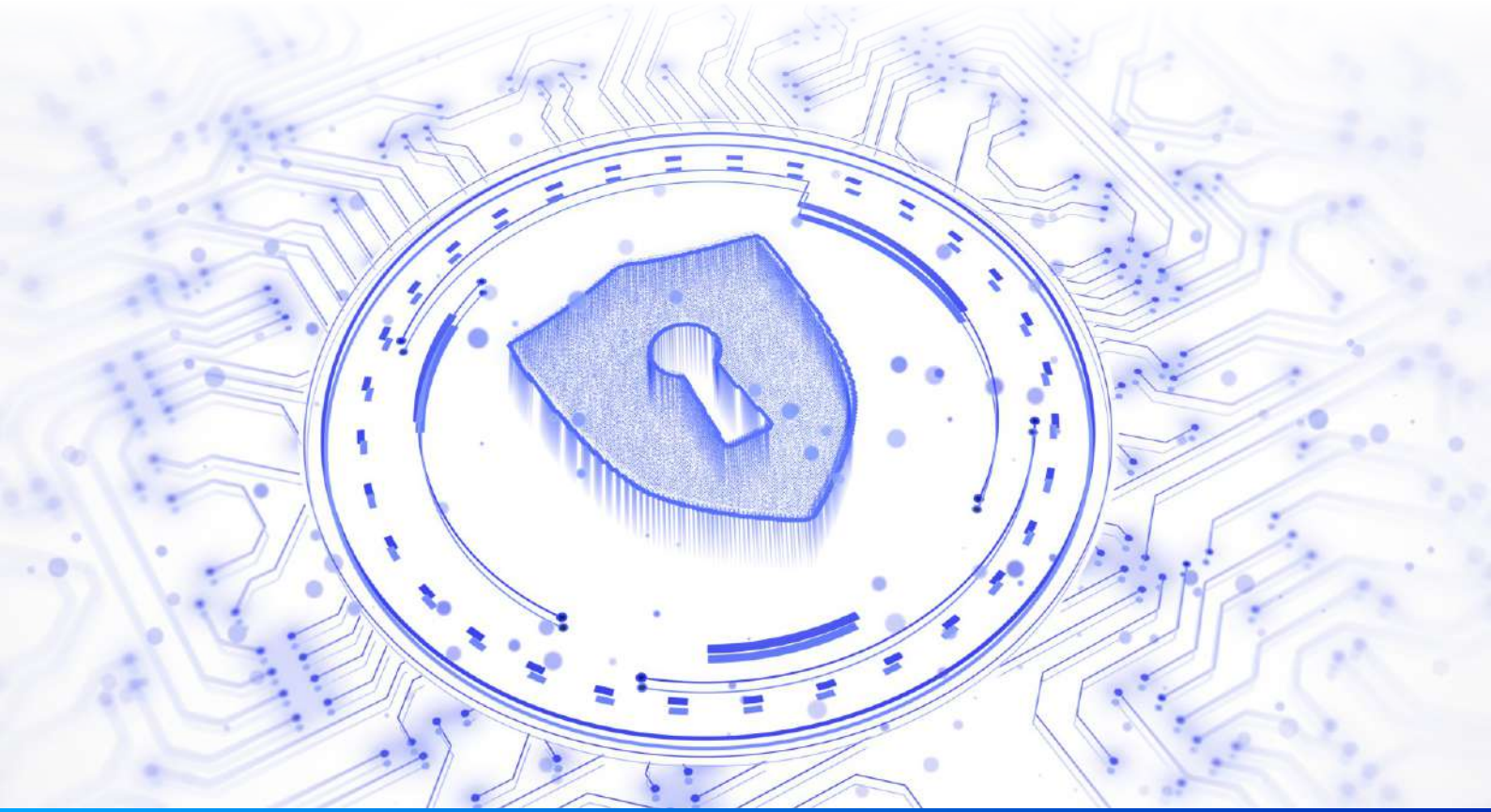
It vindicates the fact that MSPs are always in the crosshairs of cybercriminals, because by targeting MSPs, cybercriminals can access many other organizations, opening the opportunity for them to penetrate the associated customers' networks.

Therefore, any form of supply chain attack on MSP can lead to widespread chaos involving many organizations, causing more damage than a regular supply chain attack.

Take SimpleHelp, for example, its RMM software product has thousands of customers spread across the globe. Through a single hack, hackers were able to target multiple organizations.

To make matters worse for MSPs, they face challenges from multiple directions whether it is rising competition, increasing complexity of cybersecurity solutions, widening skills shortage in cybersecurity, or meeting the changing compliance requirements.

For MSPs to grow in today's business world, it has become critical for them to proactively build resilience and improve compliance.



MSPs in the world of cyber threats

MSPs are the enablers of digital transformation, providing key IT services like cloud, networking, data, and other services. However, the thing that makes them the enablers of digital transformation also makes them a viable target for cybercriminals.

As cybersecurity experts and cyber criminals try to win the arms race, MSPs face an increased threat of operational disruption, loss of data, and reputational damage. Attackers targeting edge devices are coming up with evolved forms of ransomware that could go undetected by or evade EDR.

Non-traditional threats, like AI-based phishing and deepfake attacks, pose a greater threat to MSPs as they don't easily get detected by threat detection systems.

Let us explore some of the primary challenges identified by cybersecurity experts for MSPs in the world of cyber threats.

01. Primary challenges to MSPs in the world of cyber threats

- Advanced AI powered cyber threats

MSPs are struggling to keep up with sophisticated AI-powered threats, especially sophisticated threats like AI-powered cyber threats that are not just difficult to detect but also highly persistent.

How cybercriminals use AI

01 Hackers create zero-day malware using AI that can automatically exploit undiscovered security weaknesses.

02 They use malicious AI-based attacking tools that assist them in maintaining persistence and masking their presence in the network.

03 They use AI/LMM-based tools available in the dark marketplace (like Fraud GPT) that help them create phishing campaigns or create malware with a unique strain that is challenging to detect

04 Hackers can position data sets to skip detection of specific security weaknesses or give false data.

05 Using AI, they automatically detect security gaps in vendor/third-party environments to orchestrate third-party attacks.

06 They use LLM solutions like ChatGPT to quickly gather publicly available information or OSINT (Open Source Intelligence) on their targets to carry out tailored phishing campaigns.

- Targeted attacks
In the past three years, there has been a considerable rise in targeted attacks on MSPs.

It is primarily because a majority of MSPs, especially SMBs, have less mature defenses with lots of undiscovered vulnerabilities. By targeting MSPs, they can target a wider network of organizations connected to them.

The recent ransomware attacks based on the exploitation of vulnerabilities in RMM software, SimpleHelp, namely CVE-2024-57727 (path traversal vulnerability), CVE-2024-57728 (arbitrary file upload flaw), and CVE-2024-57726 (privilege escalation flaw), allowed hackers to target every MSP/business using the software.

The exploitation allowed attackers to further exfiltrate data and use Dragonforce ransomware to encrypt their data.

- Advanced social engineering attacks
Cybercriminals are using advanced social engineering techniques to target MSPs and businesses. They use methods like fake CAPTCHA where the victim is redirected to a malicious CAPTCHA that deploys an infostealer (like Lumostealer) on their systems to steal their data.

There is a rise in QR-based phishing or Quishing scams where attackers steal data or deploy malware by posing as a representative from Microsoft, asking their victims to scan a malicious QR to log in to their Microsoft 365 account. Another form of attack where attackers bypass MFA is the Evilginx attack, where the attackers use a phishing tool to target Microsoft Entra ID users to steal their credentials.

How an Evilgnx attack works

01 An attacker generates a malicious link that takes the victim to his server that runs Evilginx (the victim gets redirected to his proxied sign-in page. For example, a document hosted on Google Drive).

02 The attacker sends the target/victim their likeness through email, messenger, text, etc.

03 The victim clicks on the link.

04 The victim is taken to the Google sign-in page proxied by Evilgenix.

05 The victim enters the account details, progresses MFA, and is redirected to the malicious URL initially created by the attacker.

06 The attacker has the credentials (email ID and password) and session cookies of his victim that he can use to take full access/control of the victim's account bypassing 2FA protections enabled.

- Evolved ransomware attacks

Just as MSPs enable organizations with their services, RAAS (Ransomware-as-a-service) providers enable attackers with unique and more persistent strains that automatically encrypt sensitive information after exploiting the security vulnerabilities in their victims' environment.

The small size of MSPs makes them an attractive target compared to a large organization that has high levels of security. Even MSPs that have deployed a hygiene level of security aren't safe from such evolved attacks. Attackers are leveraging AI to come up with lethal ransomware attacks that can even evade detection from EDR.

MSPs face an increased threat from the newly emerging threats that utilize the deadly combination of ransomware and AI. It is a major reason behind the increase in the frequency of attacks on MSPs, leaving some out of business.

02. Business challenges

The global cybersecurity skills shortage is predicted to rise by 19.1% per annum (ISC2). MSPs are struggling with limited expertise in cybersecurity, having to rely on multiple vendors to meet their cybersecurity and compliance needs.

Over time, cybersecurity solutions evolve to keep up with the threats, and they also will become more complex to manage and costlier to afford. Gartner has predicted that leaders will have to find a way to consolidate and manage solutions from different vendors post-2025.

03. How can MSPs stay proactively ahead of and prepared for cyber threats?

As AI makes it easier and quicker for cybercriminals to carry out attacks, they utilize AI-based tools for phishing, exploitation of vulnerabilities, and spreading malware.

MSPs are under increased pressure to secure their infrastructure, data, and reputation all while keeping up with changing compliance requirements. It can be a struggle balancing between cybersecurity and compliance.

Dealing with evolving threats alone can be a challenge for MSPs, especially with limited expertise, insufficient resources, and siloed solutions. It calls for partnership with a cybersecurity vendor that can provide the needed expertise to ensure round-the-clock security of information assets and operations of the business and clients.

04. How can collaborating with a cybersecurity vendor help MSP'sbusiness and clients?

01

Dedicated expertise -
MSPs can get dedicated expertise to configure, manage, and monitor their solutions.

02

Enhanced productivity -
it can free their teams to focus on critical IT tasks and improve their productivity.

03

Reduced security and compliance risks -
With dedicated experts looking over their security and compliance, they can reduce their cyber risks and non-compliance considerably.

04

Saved time and cost -
by getting cybersecurity experts to work on their infrastructure's security, they can reduce the cost associated with security risks and non-compliance.

MSPs in the realm of compliance

Since MSPs are providers of IT services to key digital/IT services to organizations, any cyber attack could threaten not just their operations but also the organizations they deliver services to, including critical industries that rely on their services.

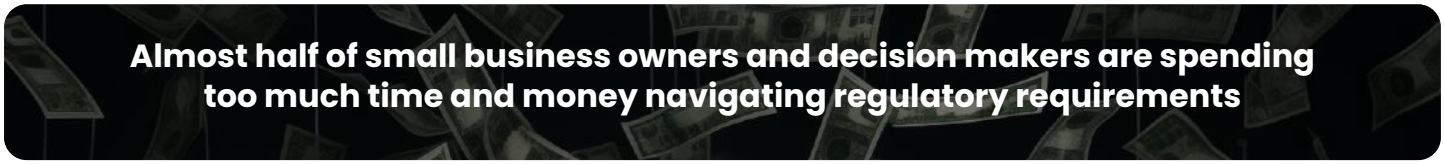
Therefore, MSPs are subjected to some of the key global regulations, certifications, standards, and frameworks, including HIPAA, ISO 27001, CMMC, PCI DSS, and GDPR.

However, they struggle to ensure security and compliance with the regulations because of the rising frequency of threats like ransomware and data breaches that threaten their operations, data, and reputation.

As these threats constantly evolve, compliance regulations keep changing, becoming more complex with cross-border laws growing stricter, requiring MSPs to timely monitor these developments and prepare/adjust their compliance strategies accordingly.

Due to a rise in competition, compliance has become a key differentiator for MSPs, especially certifications like ISO27001 that have become key elements that boost trust among customers and prospects.

Therefore, MSPs are under increased pressure to improve their compliance and adhere to the regulatory requirements applicable to them.



Key challenges

01. Balancing time and resources for compliance

MSPs can struggle balancing time and resources for security audits and compliance alongside core operations. Compliance activities demand sparing time and allocating resources to ensure that they accurately meet the requirements. However, teams struggle to balance their workloads, often having a limited bandwidth for compliance activities (audit, documentation, etc.)

How can it be solved?

Through AI, all the time-consuming compliance tasks can be automated, and AI-based compliance monitoring can be done using playbooks designed by security and compliance experts, saving both time and resources.

02. Keeping up with changing compliance environment

Whether it is the enactment of new laws, introduction of new frameworks, or a change in existing regulations, managing change can be a challenge as an MSP especially when dealing with multiple regulations and frameworks. As compliances grow in complexity, MSPs can struggle to keep up with the changing compliance environment.

How can it be solved?

It can be solved by collaborating with a compliance expert who has the right subject matter expertise with specific regulations (like PCI DSS, HIPAA, GDPR, ISO27001, NIST, etc).

03. Documentation

Ensuring accurate and timely documentation of policies, procedures, and technical controls can be a challenge as an MSP, especially with a small team with limited bandwidth from IT support operations.

How can it be solved?

Through a centralized platform that manages all the compliance-related documents and performs evidence collection ensuring that there is nothing goes amiss and ensures timely documentation.

04. Training and awareness

Regulations, certifications, and frameworks require organizations to engage in regular training and awareness of security and privacy best practices specific to their roles. However, MSPs struggle to ensure that compliance is a priority for teams that see it as an administrative burden, aligning staff's understanding of their compliance roles, and tracking and ensuring that employees have engaged in training.

How can it be solved?

MSPs must prepare a detailed plan, develop a mechanism to periodically measure the awareness levels of employees, and establish a reward mechanism that encourages employees to be more compliant.

Plausible solutions for MSPs

A major challenge that almost all MSPs face while trying to navigate cybersecurity and compliance of their business and customers is that a majority of vendors offer expertise only in cybersecurity or compliance but rarely both. It raises the dependency on multiple vendors for security.

It is not only time-consuming but also involves spending lots of money, SharkStriker helps MSPs solve this by offering dual expertise in cybersecurity and compliance, assisting MSPs in proactively identifying and addressing cybersecurity and compliance gaps of their business and customers.

MSPs can manage the risk and compliance of clients through SharkStriker's white-labelled managed services including comprehensive assessments using VAPT, Attack Surface Monitoring, and Red teaming. They can offer detailed recommendations based on holistic assessments to improve resilience and achieve Governance, Risk, and Compliance goals.

White-labeled Managed Services

01. Compliance centric MDR services

- A bundled human-led tech-driven offering delivered via SharkStriker's purpose-built security platform STRIEGO.

- 24x7 Security Monitoring by SOC
- STRIEGO MDR Platform with SIEM (multi-tenant, multi-tier)
- Network Detection & Response (NDR)
- Full-Cycle Incident Response
- Host-Based Vulnerability Assessment
- Network Vulnerability Assessment (Internal & External)
- Annual Network Penetration Testing
- Security Audit of Controls (EDR, EPP, Cloud)
- Security Advisory & Posture Review
- Multi-Sourced Threat Intelligence
- Third-Party Tool Integration
- Weekly & Monthly Security Reports

02. Managed SIEM services

- Round the clock management and configuration of SIEM with industry best practices for optimal performance, seamless detection and high ROI outcomes from SIEM.

- Design and provisioning
- Use case management
- Detection, Response & Investigation
- Risk & Compliance Management
- STRIEGO – multi-tenant, fully hosted, and managed security platform with in-built UEBA & SOAR

03. SOC-as-a-service

- 24/7 access to specialized cybersecurity and compliance expertise, including security analysts, incident responders, threat hunters, threat researchers, DevSecOps engineers, and domain experts for high ROI outcomes from the existing security suite.

- 24x7 Monitoring & Response of status quo controls
- IR – Comprehensive guidance for action
- Monthly Security Posture Review
- Threat Advisory
- Threat Intelligence
- Complementary 3rd party integration
- Weekly & Monthly reports

04. Pentesting services

- Comprehensive assessment of risks and strength across infrastructure (including network, web API, IoT & Mobile apps) using the most offensive automated and manual real-word attack methods used by modern-day cybercriminals.

- Continuous pentesting against top critical and emerging vulnerabilities (MITRE, CWE, OWASP Top 10, and SANS 25
- Detailed report of all the security weaknesses with security recommendations to treat them
- Categorization of risks based on priority, severity, and Proof of Concepts of risks
- Testing against 2000+ case scenarios
- End-to-end support with vulnerability discovery and remediation
- Compliance-friendly reports throughout the process (for standards like GDPR, HIPAA, PCI DSS, and ISO27001)
- Certified pentesters and threat experts
- Certification of security audit

05. Red teaming

- Assessment of preparedness of status quo defense through simulation of real-world attacks where SharkStriker's red team identifies gaps in existing capabilities, security measures, procedures, controls etc.

- Expert-led risk analysis
- Impact assessment
- Technical assessment as per posture
- A multi-dimensional approach to testing
- Intelligence-based attack methods
- Detailed recommendations to boost cyber resilience and preparedness of security team
- Comprehensive reporting

06. Attack Surface Management (identities, external and internal attack surface management)

- Identification and management of risk across digital identities, internet facing assets, and internal infrastructure for exposure to risks or compromise.

- Proactive treatment of risks through severity and priority-based categorization
- Insights on external attack surface hygiene
- Vendor risk profile
- Risk scores based on risk exposure
- Data leak detection

07. 360 degree compliance management

- SharkStriker offers dedicated compliance expertise to proactively identify and address compliance gaps to comply with applicable regulations, standards, frameworks, and certifications.

- Comprehensive gap assessment
- Preparation of risk treatment plan
- Implementation with complete assistance with technological deployment
- Assistance with external audit
- Extensive post-implementation review
- Add-on services

SharkStriker Partner Program

- A unique program tailored for MSPs and business owners to grow business in cybersecurity by leveraging SharkStriker's high-revenue, zero-investment white-labeled offerings.

- White-labeled cybersecurity services
- White-labeled security platform, SOC, sales team
- Dedicated marketing, sales, technical support
- Flexible program - Distributor/Reseller/Referrel/MSP Partner

Sources

01. Verizon's Databreach Investigations Report 2025
02. Vikingcloud - 2025 SMB Threat Landscape Report
03. https://sharkstriker.com/blog/cybersecurity-predictions-for-2025/
04. Q4 MetLife & US Chamber of Commerce Small Business Index
05. https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025
06. Zscaler Threatlabs phishing report

SharkStriker

1990 N California Blvd Suite 20,
Walnut Creek, CA 94596, USA

+1 925 5321900

sales@sharkstriker.com

www.sharkstriker.com