restorepoint
A ScienceLogic company

SOLUTION BRIEF

Network and Security Compliance for MSPs: What Leadership Needs to Know

Managed service provider (MSP) CEOs face many challenges. Reseller trade journal CRN asked several MSP CEOs what the biggest challenges to the future success of their businesses were, and four themes appeared repeatedly in responses:

- Keeping existing tech running amid supply chain challenges
- Differentiation in a highly competitive market
- Maintaining security and cyber hygiene
- Hiring and retaining IT talent

Those concerns are magnified in the MSP market, which is experiencing rapid growth and is forecast to grow from $243 billion in 2021 to nearly $355 billion by 2026. To successfully address each challenge means improving technical operations to emphasize operational resilience, reliability, and compliance.

$243 billion in 2021

$355 billion by 2026

$112 billion

rapid growth forecasted in the MSP market by 2026

ScienceLogic's Restorepoint network configuration backup, recovery, compliance analysis, and change management solution can play a crucial role for MSPs. Here's how.

- Compliance Management Makes Business Sense
- Why Compliance is Essential for MSPs
- The Importance of Thorough and Reliable Compliance Management
- Four Compliance Best Practices for MSPs
- Five Questions to Ask Before an Incident Occurs
- ScienceLogic Restorepoint Can Help

Compliance Management Makes Business Sense

Cybersecurity isn't just about preventing cyberattacks and avoiding data breaches; it is also about complying with the many security and privacy regulations that dictate how various kinds of sensitive data—like financial, healthcare, personal, and intellectual property—are protected and managed. Compliance builds trust, and brand trust translates to a competitive edge.

Whether an MSP focuses on a specific network segment like healthcare, retail, or financial services, there are many local, nation, international, and industry regulations and standards that must be met and managed to gain customer trust and avoid penalties for non-compliance. Here's a list of some key regulations and standards from across the globe:

46%

of European managed service providers are concerned about security issues.

Country	Standard / Rule
Australia	APRA CPS 230
Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)
EU	EU Digital Operational Resilience Act (DORA)
EU	General Data Privacy Regulation (GDPR)
EU	Payment Services Directive 2 (PSD2)
Hong Kong	Supervisory Policy Manual—Operational Resilience
Luxembourg	CSSF 21/787 Major Incident Reporting
Singapore	Guidelines on Business Continuity Management
South Africa	D4-2023 Directive on Operational Resilience
Switzerland	FINMA Circular 2023/1 Operational risks and resilience
UAE	DFSA AMI 5.5
UK	Data Protection Act (DPA)
UK	Financial Conduct Authority SYS 15A.2
US	Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers
US	Gramm-Leach-Bliley Act (GLBA)
US	Banking Secrecy Act (BSA)
US	Federal Financial Institutions Examination Council (FFIEC) Guidelines
US	NIST Cybersecurity Framework
US	Sarbanes-Oxley (SOX)
Industry Standard	Payment Card Industry Digital Security Standard (PCI DSS)

Why Compliance is Essential for MSPs

In May of 2022 the U.S. Cyber & Infrastructure Security Agency (CISA) and FBI issued a joint advisory with their "Five Eyes" peers in Australia, Canada, New Zealand, and the UK warning of threats specific to MSPs, recommending that customers contractually obligate their MSP partners to demonstrate security compliance.

While certifications are a useful compliance proof point, the test is in delivering a high quality of service, and MSPs that fail to meet expectations will be left behind.

Furthermore, corporate executives are now on notice and may be held personally liable for the consequences of their companies' failures to meet compliance demands. In 2023 in a precedent-setting case, a former Uber CISO was sentenced to three years' probation for failing to disclose a breach and for felony obstruction.

The Information Systems Audit and Control Association (ISACA) recommends that corporate management focus on six areas of focus for compliance oversight:

1. Employee awareness
2. Risk assessment
3. Patching
4. Compliance
5. Audits
6. Incident reporting

> "Cybersecurity oversight has now become the most important topic for the Board after strategic planning."
>
> **2021 Deloitte: The Changing Role of the Board on Cybersecurity: Robust oversight "Now" for a secure "Next"**

Common Technical and Professional Certifications & Standards

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- Certified Information Privacy Professional (CIPP)
- Certified Information Security Manager (CISM)
- ISO 27001
- Payment Card Industry Digital Security Standard (PCI-DSS)
- NIST Cybersecurity Framework
- System & Organization Controls 2 (SOC2)
- Network and Information Security Directive 2 (NIS2)

The Ponemon Institute/IBM 2023 *Cost of a Data Breach Report* found the average cost of a data breach to organizations was $4.45 million per incident. Specific industry results differ widely.

The Importance of Thorough and Reliable Compliance Management

Maintaining a security and network compliance program is a daunting task for MSPs that are responsible for their own systems as well as their customers. Without automation, vast amounts of costly human effort are required to perform checks to ensure that internal or customer network configuration and compliance policies are met. By automating compliance checks, Restorepoint can not only cut staff time dedicated to such tasks by more than 50%, but can perform those checks on a daily basis alongside the backup process, dramatically reducing the potential of breaches caused by misconfiguration or intrusion that might be undetected between manual audit cycles.

Four Compliance Best Practices for MSPs

For MSPs that want to minimize the risks associated with a data breach and associated fines for regulatory non-compliance, we recommend four best practices:

1. Actively track, verify, and manage system and configuration changes centrally.
2. Build, manage, and automate compliance checks that increase security and help demonstrate capabilities to auditors and customers.
3. Ensure a failsafe mechanism to be able to automatically restore configurations to compliant versions.
4. Eliminate the operational silos that exist when managing multiple network technologies and customer environments.

ScienceLogic Restorepoint Can Help

Having the right tools in place to automate repetitive and programmatic processes like audits and backups is vital to ensuring that network compliance is fast, accurate, and fully documented. When left to traditional manual work, the risks and costs are far too high.

ScienceLogic's Restorepoint solution automates many of the steps required for network compliance and change management, saving as much as half of their time by shifting from repetitive, manual tasks and an average of 15,000 total labor hours per year—and with better results.

Contact ScienceLogic for more information.

Five Questions to Ask Before an Incident Occurs

To help prepare and prioritize a compliance plan, ScienceLogic's Governance, Risk, and Compliance experts recommend that leadership ask five revealing questions:

1. Is our network risk quantified and appropriately prioritized?
2. Is our backup strategy centralized, robust, and fit for purpose?
3. What are our current incident response times for outages or breaches?
4. How are our compliance obligations being managed?
5. What's the cost to the business if an incident shows we don't meet our customers security or availability requirements?