

Navigating the Cybersecurity Storm

Urgent Imperatives for MSPs



The cybersecurity landscape is in a state of flux, with new challenges emerging in the form of increased ransomware attacks, heightened scrutiny from legal entities, and rigorous regulatory standards. Managed Service Providers (MSPs) are now operating in an environment where cyber insurance premiums are on the rise, mainly due to the surge in ransomware incidents. Companies are compelled to strengthen their cyber defenses not only for enhanced security but also to ensure the affordability of cyber insurance. The legal dimension has also taken a sharp turn, as evidenced by the SEC's recent charges against SolarWinds and its CISO, highlighting the gravity of personal and corporate liabilities. Furthermore, the introduction of the Cybersecurity Maturity Model Certification (CMMC) standards by the Department of Defense (DoD) and Department of Homeland Security (DHS) is reshaping industry benchmarks and imposing more rigorous requirements on MSPs.

The imperative for MSPs is clear: adapt swiftly to these market dynamics to mitigate risks and maintain compliance.

For MSPs, the time to act is now.

Triple Threat in Cybersecurity: Cyber Insurance, Legal, and Regulatory-Driven Urgency

- 1. Cyber Insurance Evolution:** As ransomware threats escalate, cyber insurance becomes more critical and costly. Companies must now enhance their cybersecurity measures to qualify for reasonable premiums. This shift drives a new standard for cyber readiness as insurers adjust policies to address the growing risk.
- 2. Legal Precedents with Real Consequences:** The SEC's recent charges against SolarWinds and its CISO after the significant breach reveal a landscape where legal accountability intensifies. This highlights the dual risk of personal and corporate liabilities, establishing a legal precedent that demands vigilant cybersecurity practices.
- 3. Regulatory Reformation via CMMC:** The DoD and DHS are now enforcing the CMMC standards, introducing stringent benchmarks for cybersecurity maturity. Organizations must navigate and conform to these evolving requirements, shaping the cybersecurity industry and influencing security strategies across sectors.

Pivotal Cybersecurity Vulnerabilities to Mitigate

1

RANSOMWARE PREPAREDNESS FOR CYBER INSURANCE:

Strengthen defenses against ransomware to meet cyber insurance criteria and control premium costs.

2

LEGAL COMPLIANCE WITH ACCESS PROTOCOLS:

Align password and access management policies with legal standards to avoid liabilities.

3

REGULATORY-GRADE ACCESS CONTROLS:

Implement access controls that meet or exceed regulatory requirements to protect against unauthorized entry.

4

DATA GOVERNANCE FOR COMPLIANCE:

Manage and monitor sprawling data effectively to comply with stringent regulatory expectations.

5

SECURE COLLABORATION TO MITIGATE LEGAL RISKS:

Adopt secure data-sharing protocols to uphold integrity in collaborative, multi-user environments and reduce the risk of legal repercussions.

Egnyte's Role in Navigating the Triple Threat in Cybersecurity: Tailored Solutions for MSPs

Egnyte's cybersecurity solutions are at the forefront of combating the increasingly sophisticated threats facing today's digital infrastructure. By offering a comprehensive suite of tools, Egnyte empowers you to not only confront these challenges but also to turn them into opportunities for reinforcing their security posture:

- **Enhanced Data Security and Governance:** Egnyte's Data Security and Governance services are pivotal for maintaining rigorous data oversight and implementing nuanced access controls. These measures are crucial for mitigating risks linked with data sprawl and the complexities of collaboration, ensuring alignment with evolving industry standards, and tightening regulatory and cyber insurance requirements.
- **Alignment with CMMC 2.0 Standards:** Egnyte's suite of CMMC solutions is designed to help navigate the intricate requirements set forth for defense contractors, ensuring the protection of sensitive government data. These tools provide a pathway for MSPs to confirm their adherence to the stringent cybersecurity benchmarks mandated by the DoD and DHS, safeguarding their clients' contractual standing and competitive advantage.

- **Robust Ransomware Recovery:** As ransomware becomes increasingly prevalent, Egnyte's Snapshot Recovery emerges as a critical tool for organizations to rapidly restore data to its state before an attack. This capability is particularly valuable in today's market, where cyber insurance plays a significant role. Cyber Insurers emphasize the need for robust recovery solutions as part of the risk assessment process, which can affect coverage terms and premium costs. Egnyte's Snapshot Recovery not only expedites the restoration process but also serves as a proactive measure, potentially lowering insurance premiums by demonstrating comprehensive risk management strategies that minimize the potential impact of ransomware attacks.

Egnyte's cybersecurity offerings are more than just defenses; they represent a proactive ethos, enabling MSPs to shift from reacting to threats to preemptively addressing them. This proactive stance, supported by Egnyte's solutions, empowers MSPs to improve service delivery and establish themselves as anticipatory security leaders in a dynamic digital landscape.

The Imperative for MSPs

1. **Prioritize and Secure:** Make cybersecurity your top priority, protecting your customers' data against all potential threats.
2. **Educate and Engage:** Elevate awareness among your customers about the rising legal and regulatory demands.
3. **Implement and Innovate:** Take a proactive stance with Egnyte's solutions to fend off current and future cyber threats.
4. **Differentiate and Deliver:** Distinguish your service offerings by demonstrating a deep commitment to data security and regulatory compliance.
5. **Stay Ahead of the Curve:** Lead with Egnyte to stay ahead in cybersecurity with their thought leadership and innovations.

In an era where cybersecurity is under the microscope of insurance underwriters, legal frameworks, and regulatory bodies, MSPs must elevate their security strategies to new heights. Cyber Insurance is now a critical piece of the cybersecurity puzzle, influencing how MSPs architect their defenses to ensure insurability and manage premiums. Egnyte's suite of solutions offers the tools and support MSPs need to navigate this complex terrain. By enabling robust data security measures, compliance with the latest legal expectations, and adherence to rigorous regulatory standards, Egnyte positions MSPs to meet and exceed the multifaceted demands of today's cybersecurity landscape, ensuring compliance and peace of mind.



Immediate Action Required: Elevate Your Cybersecurity Now

Don't wait for the threat to become a reality. Join forces with Egnyte today to fortify your cybersecurity posture. Enhance your defenses, assure compliance, and stay at the forefront of the industry. Secure your operations and secure your customers' data - because in the realm of cybersecurity, tomorrow is one day too late.

**Empower Your Security, Empower Your Future —
With Egnyte, Tomorrow's Security is Today's Priority.**

TAKE ACTION NOW!

EGNYTE | PARTNER PROGRAM

Egnyte is the secure multi-cloud platform for content security and governance that enables organizations to better protect and collaborate on their most valuable content. Established in 2008, Egnyte has democratized cloud content security for more than 26,000+ organizations, helping customers improve data security, maintain compliance, prevent and detect ransomware threats, and boost employee productivity on any app, any cloud, anywhere. For more information, visit www.egnyte.com/partners.

Contact Us

US: +1-650-968-4018
EMEA – UK: +44.020.3356.3714
www.egnyte.com