Overcoming Federal Sector Compliance Regulation Challenges

Skyhigh Security's Nick Graham on How Technology Can Help Meet Compliance Demands

Nick Graham

Graham has more than two decades of experience. He has developed an extensive knowledge of cybersecurity best practices and technologies throughout his career, successfully implementing and managing complex security programs for a variety of organizations. His expertise spans multiple domains, including risk management, compliance, incident response, threat intelligence and security operations. He has worked with clients from a diverse range of industries, including financial services, healthcare, government and technology, and has delivered innovative security solutions that have protected critical assets and data from cyberthreats.

The sheer volume of federal regulations in place makes it almost impossible for agencies to monitor and comply with all of them, much less understand the impact of new ones.

In the second installment of this podcast series by Skyhigh Security on data protection, **Nick Graham**, senior solutions architect for the public sector at Skyhigh Security, explored the many compliance challenges – and how to overcome them.

“One of the possible solutions is to leverage technology to simplify compliance regulation,” Graham said. “Security software, for instance, can help federal agencies identify and monitor compliance requirements, then track the compliance metrics and automate the compliance or remediation process. This can help reduce the burden of compliance regulation and ensure that agencies are in compliance with the latest regulations.”

In this podcast with Information Security Media Group, Graham discussed:

- Why there are so many compliance challenges in the face of a trend toward greater accountability;
- How the latest software technologies can help solve these challenges;
- What the future holds for the regulatory and political environments.

> **“In the context of cybersecurity, compliance regulations usually provide a framework for organizations to manage and protect their data and information systems and assure that they meet security standards.”**

Federal Government Compliance Regulation

CAL HARRISON: Let’s start with some background: What is compliance regulation in the federal government?

NICK GRAHAM: Compliance regulation in the federal government refers to the set of rules, guidelines and standards that organizations must follow to ensure security and protection of sensitive information for cyberthreats. In the context of cybersecurity, compliance regulations usually provide a framework for organizations to manage and protect their data and information systems and assure that they meet security standards.

National Cybersecurity Strategy

HARRISON: The Biden administration released a national cybersecurity strategy that calls for mandatory compliance with federal standards. What are the implications for agencies and organizations that have to comply with these regulations?

GRAHAM: I’m glad to see that the administration is starting to focus on that. The national cybersecurity strategy that Biden released outlines several mandatory compliance requirements for federal agencies and organizations. These regulations are designed to strengthen the nation’s cybersecurity posture and protect against cyberthreats and attacks.

The implications for agencies and organizations that have to comply with these regulations are significant. They’ll need to invest in resources and infrastructure to meet the required standards and ensure that their systems and networks are secure. There will be a need for increased training and education for their employees to ensure that they’re aware of the cybersecurity risks and how to mitigate them. Those organizations will also need to conduct regular assessments and audits to ensure that the training is working and that they are compliant with the regulations.

Noncompliance could result in significant consequences, including financial penalties and reputational damage, and could leave organizations vulnerable to cyberattacks and breaches, which could result in data loss, theft or even worse. The mandatory compliance requirements outlined in the national cybersecurity strategy represent a significant shift toward a more robust and proactive approach to cybersecurity, which is crucial in today's rapidly evolving threat landscape.

Challenges of Complying With Regulations

HARRISON: What are some of the challenges of protecting data and complying with federal regulations?

GRAHAM: One of the most significant challenges is the sheer number of regulations that federal agencies are required to comply with. Another challenge is that agencies need to do more with less. Compliance regulation requires a significant amount of time, money and manpower, and many agencies simply don't have the resources to devote to it. Another significant challenge is the complexity of the regulations. Many of them are highly technical and difficult to understand, making compliance challenging for agencies that are not well-versed in the subject matter. Also, regulations can change frequently and agencies must constantly update their compliance procedures to ensure they are in compliance.

HARRISON: Why do these challenges exist?

GRAHAM: Regulations are often created in response to specific events or incidents, and they may not be well-thought-out or easy to implement. Also, regulations are often created by different agencies and departments, leading to inconsistency and confusion. And compliance regulation is often viewed as a burden rather than a benefit. Many agencies view it as a drain on their resources rather than as a way to protect the public and the environment.

Addressing the Challenges

HARRISON: What can be done to address these challenges?

GRAHAM: One of the possible solutions is to leverage technology to simplify compliance regulation. Security software, for instance, can help federal agencies identify and monitor compliance requirements, then track the compliance metrics and automate the compliance or remediation process. This can help reduce the burden of compliance regulations and ensure that agencies are in compliance with the latest regulations. Also, providing more resources to agencies – such as more funding for additional training for staff – can help improve compliance outcomes. Finally, accountability is the crucial piece in ensuring compliance. Agencies should face significant consequences – including fines and penalties – for failing to comply with regulations. This would go a long way to ensure that agencies prioritize compliance regulations and take them seriously.

> **“Cybersecurity is an ongoing process. You can’t just sit there, take one stance and think that you’re going to be done. Attacks are always increasing in frequency, sophistication and impact. So always stay ahead of them.”**

The Future of Compliance Regulation

HARRISON: What does the future hold for compliance regulation?

GRAHAM: The future of compliance regulations in the federal government is uncertain due to changes in leadership and priorities. When one administration replaces another, there may be shifts in focus on and enforcement of regulations. Also, technology is moving at such a rapid pace and the industries are evolving. As new technologies emerge, new regulations will need to be developed to address the emerging risks and challenges. There also may be efforts to streamline regulations and reduce the burden on agencies. But regardless of the future direction of compliance regulations, it is clear that they will continue to be a critical aspect of ensuring public safety, health and protection in the federal government.

FedRAMP and Impact Level 5 Certifications

HARRISON: What is Skyhigh Security doing to address compliance regulations, and what do you see when you work with your clients?

GRAHAM: First and foremost, Skyhigh Security has devoted significant time and resources to achieve FedRAMP and Impact Level 5 certifications. A company with these certifications can help organizations in several ways. FedRAMP certification is a governmentwide program that provides a standardized approach to security assessments, authorization and continuous monitoring for cloud products and services. A company with FedRAMP certification has undergone a rigorous security review process and is considered to be a trusted provider of those cloud services. It can help organizations meet compliance requirements with regard to storing and processing sensitive data in the cloud.

The Impact Level 5 or higher is a classification used by the Department of Defense to define the security requirements for cloud services handling controlled unclassified information. A company with Impact Level 5 certification has demonstrated that it meets the stringent security requirements set by the DOD for handling sensitive information. This can help organizations in the defense industry or those working with the government to meet their compliance requirements and ensure that their data is secure.

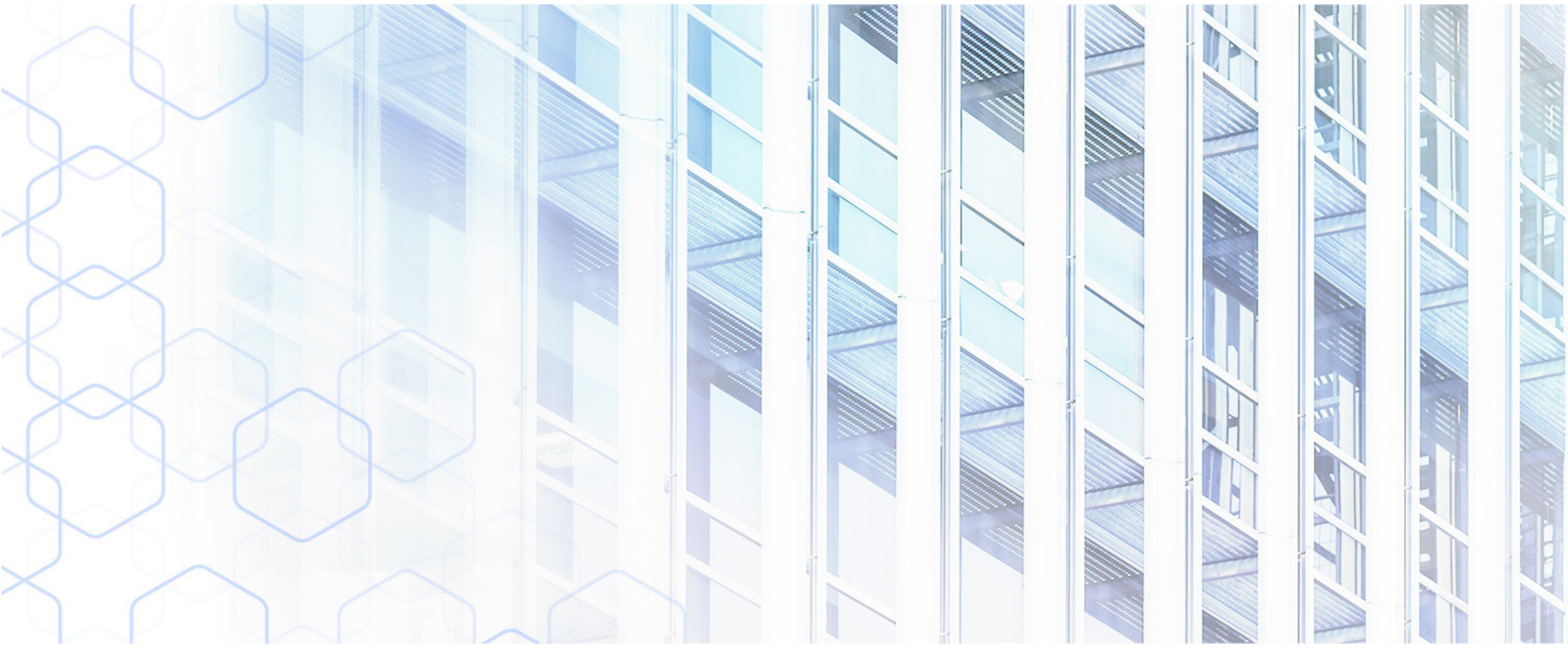
Key Takeaways

HARRISON: We've covered a lot of ground here. What are the key takeaways for our listeners?

GRAHAM: Cybersecurity threats are increasing in frequency, sophistication and impact. Organizations must prepare to detect, prevent and respond to those cyberattacks. Cybersecurity is everyone's responsibility – not just the IT department. Everybody at every stage of their day needs to take responsibility for it and make sure the threat minimizes. Compliance with federal standards is crucial. A lot of intelligent people have looked at this and provided their expertise on how to be the best protected environment possible.

Proactive measures are necessary. Don't be reactive because when you're reacting to a threat, it's already happened. Being proactive means you're getting out ahead of it and mitigating the damage. Cybersecurity is an ongoing process. You can't just sit there, take one stance and think that you're going to be done. Attacks are always increasing in frequency, sophistication and impact. So always stay ahead of them.

Skyhigh
Security



We know data. It’s who we are.

Discover Skyhigh Security for your business.

Skyhigh Security goes beyond securing data access—it secures how sensitive data is used. We extend the security control point beyond the network to the data itself. As it moves across the web to software-as-a-service applications, cloud applications and platforms, and even endpoints, we protect it with a single policy that moves with your data instead of being tied to each access technology. Our easy-to-use, integrated platform enables organization-wide data protection, streamlines data security operations, and reduces complexity.

More information at www.skyhighsecurity.com.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® Just for Credit Unions GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® Data Breach. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io