Indian Health Service

Delivering Resilient Healthcare By Mastering Cybersecurity Governance and Threat Management

PRESENTER: SOLOMON WILSON

TITLE: CYBERSECURITY PROJECT MANAGER

DATE: 08/12/2024

Introduction

01	Speaker Introduction	02	Overview of the agenda
03	What is DIS?	04	Cybersecurity A&E
05	CSIRT / CSOC	06	ISSO
07	DRCP	08	ARC
09	R&C	10	PSA

Speaker Introduction and Session Objectives

Welcome, everyone! Thank you for joining us today as we delve into a subject that touches all aspects of healthcare: Cybersecurity. Our session aims to inform and inspire action and assurance in safeguarding our most precious asset—patient data.

01 **Highlighting the Critical Importance of Cybersecurity in Healthcare.**

02 **Illustrating How the Division of Information Security (DIS) Empowers Healthcare Providers and Facilities to Protect Data and Deliver Outstanding Services Aligned with Our Agency's Mission.**

What is DIS?

Division of Information Security (DIS)

DIS, where we provide comprehensive cybersecurity services to safeguard your organization's data and systems. At DIS, we specialize in robust security architecture, effective incident response, stringent compliance assessments, and proactive risk management. Our dedicated team is committed to ensuring enterprise-level cybersecurity assurance, enabling you to focus on your core mission with confidence.

Architecture and Engineering (A&E)	Computer Security Incident Response Team (CSIRT)	Risk and Compliance (R&C)
Helps support technologies for a robust information security implementation systems.	Continuous monitoring and detection of new evolving cyber threats and response to security incidents.	Continuous system assessment for federal compliance.
Audit Response & Coordination (ARC)	**Information System Security Office (ISSO)**	**Disaster Recovery & Contingency Planning (DRCP)**
Helps streamline data calls and audit finding tracking.	Continuous monitoring and detection of new evolving cyber threats and help developing proper response and mitigations for all types of security vulnerabilities.	Secure IHS patient data, healthcare provider information, and facility management planning to meet mission essential functions (MEFs) of an organization. Also helps with BIA, developing RPOs and RTOs
Cybersecurity Vulnerability Management (CSVM)	**Cybersecurity Operation Center (CSOC)**	**Project Management Office**
Proactive protection of data integrity and availability.	Dedicated office for security enforcement and governance.	Provides assistance with implementation of security measures to modernize our healthcare technology and enhance cybersecurity in order to meet Office of Management and Budget (OMB) mandates.

Cybersecurity Architecture and Engineering (A&E)

Elevate Your Healthcare Facility's Cybersecurity with DIS A&E Services

As the healthcare industry embraces modernization and digital transformation, the importance of robust cybersecurity architecture and engineering has never been more critical. Healthcare professionals and facility managers are entrusted with the protection of sensitive patient data and the seamless operation of critical systems. The DIS Cybersecurity A&E team is dedicated to fortifying your facility's defenses through state-of-the-art security infrastructure and best practices.

Our services are aligned with risk governance protection standards described by the Cybersecurity and Infrastructure Security Agency (CISA) and National Institute of Standards and Technology (NIST) publications. By leveraging DIS A&E's expertise, your healthcare facility can navigate the complexities of new technologies and foster a secure environment for healthcare delivery.

Choose DIS A&E Services

- **Expertise and Experience:**
  - The DIS A&E team is comprised of experienced cybersecurity architects and engineers who understand the unique challenges of the healthcare sector. Our experts are proficient in the latest security frameworks and technologies, ensuring your facility is equipped with best-in-class security solutions.
- **Standards Alignment:**
  - Our services are designed in accordance with CISA guidelines and NIST standards, including NIST SP 800-53 Rev. 5 (Security and Privacy Controls for Information Systems and Organizations), NIST SP 800-160 Vol. 1 (Systems Security Engineering), and NIST Cybersecurity Framework (CSF). This alignment ensures comprehensive protection and regulatory compliance.
- **Innovative Security Solutions:**
  - We stay ahead of the curve by integrating cutting-edge technologies and methodologies into our cybersecurity strategies. From cloud security to IoT protection, our solutions are designed to address the evolving threat landscape and enhance your digital transformation efforts.
- **Customized Architectural Design:**
  - Recognizing that each healthcare facility has unique requirements, we provide tailored architectural designs that address your specific security needs and operational goals. Our solutions integrate seamlessly with your existing infrastructure and support your modernization initiatives.
- **Risk Governance and Management:**
  - Effective risk governance is the cornerstone of our approach. We help you establish and manage a robust risk framework that aligns with CISA's protective standards and NIST's risk management protocols, ensuring your organization's resilience against cyber threats.

DIS A&E Services

Security Architecture Design and Implementation

Develop and implement comprehensive security architectures that safeguard your critical systems and data. Our designs align with industry standards, including NIST SP 800-160 Vol. 1 and NIST CSF, providing a secure foundation for your IT infrastructure.

Technology Assessment and Integration

Evaluate and integrate new security technologies, ensuring they enhance rather than hinder your healthcare modernization efforts. We assess technologies such as advanced firewalls, endpoint protection, zero-trust architectures, and more.

Risk Assessment and Management

Conduct thorough risk assessments to identify vulnerabilities and potential threats to your systems. Our risk management strategies follow NIST SP 800-30 Rev. 1 guidelines, helping you mitigate risks and strengthen your cyber defense posture.

Policy and Procedure Development

Create and update cybersecurity policies and procedures that reflect best practices and regulatory requirements. We ensure that your organizational standards align with NIST SP 800-53 Rev. 5 and other relevant guidelines.

DIS A&E Services

Security Engineering and Implementation

Execute security engineering projects, from concept to deployment. Our team ensures that security controls are effectively integrated into your systems, enhancing overall operational security.

Compliance and Audit Support

Assist with compliance with healthcare regulations and prepare for audits by providing documentation and evidence of robust security practices. We help you meet requirements outlined in HIPAA and other relevant standards

Continuous Monitoring and Improvement

Implement continuous monitoring solutions to detect and respond to threats in real-time. We use advanced analytics and threat intelligence to ensure your systems remain secure against emerging threats

By Partnering with the DIS A&E Team, Your Healthcare Facility Can:

- **Strengthen Cybersecurity Framework:**
  - Establish a robust cybersecurity architecture that protects sensitive data and critical systems from a wide range of threats, supporting uninterrupted healthcare delivery.
- **Facilitate Secure Modernization:**
  - Seamlessly integrate new technologies into your operations, enhancing security while driving innovation and digital transformation in your healthcare practice.
- **Enhance Regulatory Compliance:**
  - Maintain compliance with healthcare regulations and standards such as HIPAA, avoiding legal liabilities and reinforcing patient trust in your security practices.
- **Mitigate Risks Proactively:**
  - Implement effective risk management strategies to identify and address vulnerabilities before they can be exploited, ensuring your facility remains resilient in a dynamic threat landscape.
- **Promote a Security-Conscious Culture:**
  - Foster a culture of cybersecurity awareness and best practices across your organization, empowering your staff to contribute to a secure healthcare environment.

Cybersecurity Incident Response and Threat Hunting: Strengthen Your Healthcare Facility's Cyber Resilience with DIS CSIRT Services

In the complex and dynamic landscape of healthcare, the protection of sensitive data and the continuous operation of critical systems are paramount. Healthcare professionals and facility managers are tasked with safeguarding patient information and ensuring that healthcare delivery remains uninterrupted, even in the face of evolving cyber threats. The DIS CSIRT response and Threat Hunting Team is dedicated to helping you achieve this critical mission. Our team of experts offers comprehensive services to identify, respond to, and mitigate cybersecurity incidents while proactively hunting for threats to prevent future attacks. By leveraging DIS CSIRT's expertise, your healthcare facility can fortify its defenses and ensure the safety of your patients' data.

Why Choose DIS CSIRT Services?

- **Expertise and Experience:**
  - The DIS CSIRT team consists of cybersecurity professionals with extensive experience in handling complex threats in the healthcare sector. Our experts are skilled in the latest threat detection methodologies, incident response protocols, and recovery strategies, ensuring your facility is prepared for any cyber challenge.
- **Rapid Incident Response:**
  - Time is of the essence during a cybersecurity incident. Our team provides swift and effective response services, minimizing disruption and damage. We follow best practices and industry standards to contain breaches, eradicate threats, and restore normal operations as quickly as possible.
- **Proactive Threat Hunting:**
  - Beyond reactive measures, our CSIRT team actively hunts for threats within your environment. Using advanced analytics, threat intelligence, and behavioral analysis, we identify and neutralize potential threats before they can cause harm, helping to maintain the integrity of your systems and data.
- **Customized Solutions:**
  - We understand that each healthcare facility is unique. Our services are tailored to your specific needs and environment, ensuring that our strategies align with your security goals and operational requirements.
- **Regulatory Compliance:**
  - Compliance with regulations such as HIPAA is critical for healthcare organizations. Our incident response and threat-hunting services are designed to help you maintain compliance with these regulations, protecting your Healthcare services from legal liabilities and maintaining patient trust.

Services Offered by DIS CSIRT Team

01 Utilize advanced tools and techniques to detect suspicious activity, analyze incident data, and determine the scope and impact of cybersecurity breaches.

02 Execute proven response procedures to contain the incident, mitigate its effects, and prevent further escalation. Our team works tirelessly to ensure that your critical operations continue with minimal disruption.

03 Proactively search for hidden threats within your network. By analyzing patterns and anomalies, we identify and neutralize threats that may bypass conventional security measures.

04 Conduct thorough forensic investigations to understand the root cause of incidents, collect evidence, and identify malicious actors. Our detailed reports provide insights to prevent future occurrences.

05 Review and improve your existing cybersecurity policies and procedures. We help you establish robust protocols that enhance your overall security posture.

06 Educate your staff on the latest cyber threats and best practices for incident response. Regular training sessions and simulations ensure that your team is prepared to act swiftly and effectively during a cyber incident.

07 Provide ongoing monitoring of your IT environment and recommend improvements based on evolving threats and vulnerabilities. Our adaptive strategies ensure that your defenses remain strong and up-to-date.

08 Assist in maintaining compliance with healthcare regulations by ensuring that your incident response and threat management practices meet or exceed required standards.

By Partnering with the DIS CSIRT Team, Your Healthcare Facility Can:

- **Enhance Cyber Resilience:**
  - Strengthen your defenses against a wide array of cyber threats, ensuring the continuous protection of sensitive patient data and uninterrupted healthcare delivery.
- **Respond Efficiently to Incidents:**
  - Reduce the impact of cybersecurity incidents through rapid and effective response measures, ensuring swift recovery and minimal disruption to critical operations.
- **Build Patient Trust:**
  - Demonstrate a strong commitment to cybersecurity, enhancing patient confidence in the safety and integrity of their personal information.
- **Stay Ahead of Evolving Threats:**
  - Proactively identify and mitigate threats before they can cause harm, ensuring your facility remains secure in an ever-changing threat landscape.
- **Maintain Regulatory Compliance:**
  - Ensure adherence to healthcare regulations such as HIPAA, protecting your facility from legal repercussions and maintaining your reputation.

By Partnering with the DIS CSIRT Team, Your Healthcare Facility Can:

In the high stakes world of healthcare, robust cybersecurity threat hunting engineers are vital for protecting sensitive data and ensuring continuous operation. The DIS Cybersecurity CSIRT professionals are here to provide you with the expertise, tools, and strategies needed to navigate the complexities of modern healthcare technologies securely. Our comprehensive and tailored approach, aligned with CISA and NIST standards, ensures that your healthcare service deliveries remains secure, compliant, and resilient.

Take **the next step** in fortifying your facility's cybersecurity.

Contact the DIS CSIRT today to schedule **a consultation** and discover how our services can enhance your cybersecurity threat intelligence and support your modernization efforts.

By Partnering with the DIS CSIRT Team, Your Healthcare Facility Can:

Conclusion

In the high stakes world of healthcare, cybersecurity is an essential pillar of operational success and patient safety. The DIS CSIRT and Threat Hunting Team is here to provide you with the expertise, tools, and strategies needed to protect your facility from cyber threats. Our proactive and comprehensive approach to incident response and threat hunting ensures that your healthcare organization remains secure, compliant, and resilient.

Take **the next step** in safeguarding your facility's cybersecurity. Contact the DIS CSIRT team today to schedule **a consultation** and discover how our services can help you defend yourself against cyber threats.

Information System and Security Officer (ISSO) Services Fortify Your Cybersecurity Operations with DIS ISSO Expertise

In the dynamic and high-stakes healthcare industry, robust cybersecurity operations and thorough risk management are imperative. Healthcare organizations must safeguard sensitive information and ensure continuous compliance with federal and industry standards. The DIS offers ISSO services designed to maintain and manage your cybersecurity operations, mitigate threats and vulnerabilities, and uphold compliance with Authorization To Operate (ATO) requirements. Our experienced ISSO professionals bring a wealth of expertise to strengthen your cybersecurity framework, ensuring robust protection and operational resilience.

Services Offered by DIS ISSO Team

01

Cybersecurity Operations Management:

- Oversee and manage daily cybersecurity operations, ensuring that systems and processes remain secure and efficient. Our team follows best practices and utilizes advanced technologies to protect your infrastructure.

02

Risk Management and Assessment:

- Conduct comprehensive risk assessments to identify vulnerabilities and threats. Implement risk management strategies aligned with federal guidelines and industry standards, ensuring proactive risk mitigation.

03

Authorization To Operate (ATO) Management:

- Develop, maintain, and manage ATO packages to meet federal and industry cybersecurity compliance requirements. Our ISSO team ensures that all necessary documentation and procedures are in place for secure operations.

04

Threat Detection and Response:

- Utilize advanced threat detection tools and methodologies to identify and respond to cybersecurity incidents. Our ISSO team collaborates with your IT staff to ensure timely and effective responses to potential threats.

05

Vulnerability Management:

- Implement continuous vulnerability management practices, including regular scanning, assessment, and remediation of vulnerabilities. Our approach ensures that potential weaknesses within your systems are quickly addressed

Services Offered by DIS ISSO Team

06

Policy and Procedure Development:

- Develop and enforce robust cybersecurity policies and procedures that align with regulatory standards. Our ISSO team ensures that your organization's policies support a secure operating environment.

07

Compliance Support and Audits:

- Provide ongoing support for compliance with cybersecurity regulations such as HIPAA, NIST, FISMA, and others. Prepare your Healthcare services for audits by ensuring all necessary controls, documentation, and processes are in place.

08

Security Awareness Training:

- Conduct regular security awareness training for all employees, promoting a culture of vigilance and cybersecurity best practices. Our training programs educate staff on current threats, compliance requirements, and security protocols.

09

Incident Response Planning and Execution:

- Develop and maintain comprehensive incident response plans. In the event of a cybersecurity incident, our ISSO team leads the coordination and execution of responses to mitigate impacts and restore normal operations.

10

Continuous Monitoring and Improvement:

- Establish continuous monitoring practices to keep track of security events and system integrity. Our ISSO services include ongoing evaluations and improvements to adapt to the dynamic threat landscape.

By Partnering with the DIS ISSO Team, Your Healthcare Facility Can:

Enhance Risk Management

Implement comprehensive risk management strategies to identify, assess, and mitigate potential cybersecurity threats and vulnerabilities.

1

Strengthen Cybersecurity Operations

Ensure robust management and oversight of cybersecurity operations, protecting sensitive data and maintaining efficient system functionality.

2

Proactively Manage Threats

Employ advanced threat detection and response techniques to manage and counteract potential cybersecurity threats proactively.

3

Ensure Compliance

Maintain compliance with federal and industry regulations through effective management of ATO packages and adherence to best practices and standards.

4

Maintain Operational Resilience

Build and maintain operational resilience through continuous monitoring, effective incident response, and regular improvements to security protocols.

5

Promote Security Awareness

Foster a culture of security through regular training and policy enforcement, ensuring all employees are informed and vigilant against cybersecurity threats.

6

Why Choose DIS DRCP Services Aligned with NIST Standards?

- **Expertise and Experience:**
  - The DIS DRCP group comprises highly trained professionals well-versed in NIST standards, including NIST SP 800-34 Rev. 1.
    - (Contingency Planning Guide for Federal Information Systems), NIST SP 800-53 Rev. 5 (Security and Privacy Controls for Information Systems and Organizations), and NIST SP 800-171 Rev. 3.
    - (Protecting Controlled Unclassified Information in Non-federal Systems and Organizations). Our team ensures your healthcare facility is prepared for any contingency while maintaining compliance with these standards.

- **Holistic Risk Management:**
  - We adopt a comprehensive approach to risk management, addressing both technological and environmental risks as specified in NIST SP 800-30 Rev. 1.
    - (Guide for Conducting Risk Assessments). From cyber threats like ransomware attacks to natural disasters, we help you identify, assess, and mitigate risks to maintain operational continuity.

Why Choose DIS DRCP Services Aligned with NIST Standards?

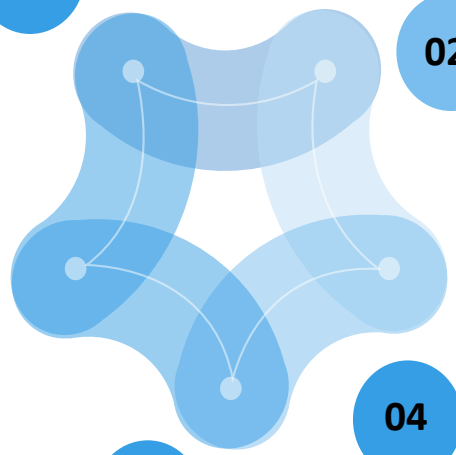
- **Customized Solutions:**
  - Understanding that every healthcare facility has unique needs, our DRCP services are tailored to your specific requirements, aligned with NIST SP 800-34 Rev. 1 and NIST SP 800-39 (Managing Information Security Risk: Organization, Mission, and Information System View). We work closely with your team to develop a disaster recovery plan that aligns with your organizational goals and operational priorities.

- **Proactive Preparedness:**
  - We believe in proactive preparedness rather than reactive measures. Our training programs, regular drills, and continuous improvement initiatives ensure your team is always prepared to handle any disruption efficiently and effectively, as outlined in NIST SP 800-50 (Building an Information Technology Security Awareness and Training Program).

Secure Your Healthcare Facility with DIS Disaster Recovery and Contingency Planning Services Aligned with NIST Standards

In the ever-evolving cybersecurity landscape in the healthcare industry, ensuring the security and continuity of operations is not just an operational requirement—it's a critical component for safeguarding patient lives and sensitive data. As healthcare professionals and facility managers, you are on the front lines, protecting your organization's information assets and maintaining uninterrupted services. The DIS DRCP group offers a comprehensive suite of services designed to strengthen your cybersecurity posture and enhance your disaster recovery capabilities. Aligned with NIST guidelines, our services elevate end-users' experience—your patients—by ensuring they receive the best outcomes even in the face of disruptions.

Key Services Offered by DIS DRCP Group Aligned with NIST Publications



01

Risk Assessment and Business Impact Analysis (BIA):

Identify critical systems and processes, assess potential risks, and understand the impact of different disaster scenarios on your operations, following NIST SP 800-30 Rev. 1 and NIST SP 800-34 Rev. 1 .

02

Disaster Recovery Strategy Development:

Develop robust backup, redundancy, and failover strategies to ensure data integrity and continuous service availability, in line with NIST SP 800-34 Rev. 1

03

Policy and Procedure Development:

Create and document comprehensive disaster recovery policies and step-by-step procedures for immediate action during incidents as per NIST SP 800-53 Rev. 5

04

Technology Implementation:

Implement state-of-the-art backup solutions, system redundancies, and cyber defences to shield your Healthcare services from disruptions, adhering to NIST SP 800-34 Rev. 1 and NIST SP 800-171 Rev. 2

05

Training and Awareness Programs

Conduct regular training sessions and simulations to build your team's readiness and response capabilities, following NIST SP 800-50 guidelines

06

Continuos Monitoring and Improvement

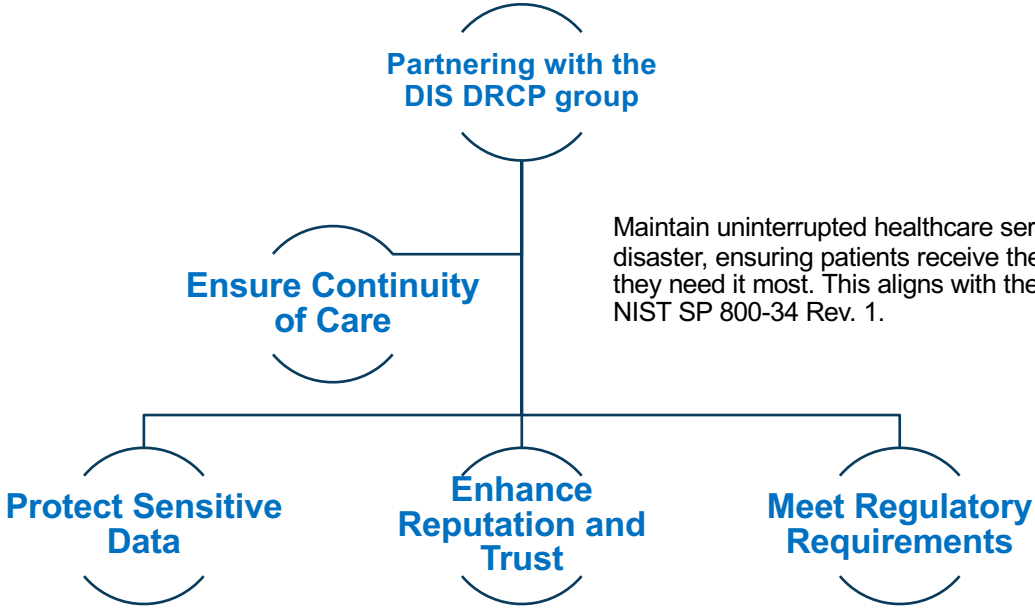
Monitor changes in the technology landscape, conduct periodic reviews, and update your disaster recovery plan to adapt to new threats and challenges, in line with NIST SP 800-53 Rev. 5

07

Compliance Assurance and Documentation

Conduct regular training sessions and simulations to build your team's readiness and response capabilities, following NIST SP 800-50 guidelines.

By Partnering with the DIS DRCP Group Your Healthcare Facility Can:



Services Provided by the ARC Group

❑ Centralized Coordination and Management:

- **Data Call Management:** The ARC group acts as the central hub for receiving and distributing data calls from Health and Human Services (HHS) and other agencies, minimizing confusion and ensuring clear communication channels.
- **Coordination of Responses:** The ARC group disseminates requirements to the right teams, consolidates responses, and submits comprehensive replies to meet deadlines efficiently.

❑ Compliance and Reporting:

- **FISMA Reporting:** The ARC group manages all aspects of the Federal Information Security Modernisation Act (FISMA) reporting, ensuring all relevant data is collected, verified, and submitted accurately.
- **Regulatory Tracking:** Keeps track of regulatory changes and ensures the organization remains compliant with all current cybersecurity and data protection laws.

❑ Plan of Action and Milestones (POA&M) Support:

- **Development of POA&Ms:** Supports the creation of detailed POA&Ms to address identified compliance gaps.
- **Monitoring and Reporting:** Continuously monitors the progress of POA&M items and provides regular updates to ensure milestones are met.

Services Provided by the ARC Group

- **Training and Support:**
  - **Staff Training:** Provides training resources and sessions to educate healthcare providers on cybersecurity best practices and compliance requirements.
  - **Technical Support:** Offers technical assistance in implementing security measures and addressing vulnerabilities.

- **Communication and Documentation:**
  - **Centralized Documentation**: Maintains comprehensive records of all data calls, responses, and compliance reports, ensuring easy access for audits and reviews.
  - **Stakeholder Communication:** Acts as a liaison between healthcare providers and regulatory agencies, ensuring clear and effective communication.

How Healthcare Providers Can Use ARC Services

❑ Reduce Level of Effort:

- **Single Point of Contact:** By centralizing data call management, healthcare providers can direct all inquiries and requirements to the ARC group, reducing the burden on their internal teams.
- **Consistent Support:** Consistent, expert support in responding to regulatory requirements means less time spent on understanding and interpreting complex guidelines.

❑ Enhance Service Delivery:

- **Timely and Accurate Reporting:** With the ARC group ensuring that all regulatory reports are accurate and submitted on time, healthcare providers can focus more on patient care and service delivery.
- **Improved Security Posture:** Through effective POA&M management and compliance monitoring, providers can enhance their cybersecurity measures, leading to fewer disruptions in service delivery.

❑ Meeting Agencies' Missions:

- **Aligned Objectives:** The ARC group ensures that all compliance and security efforts are aligned with the healthcare provider's mission and regulatory requirements, supporting overall organizational goals.
- **Resource Optimization:** By handling compliance and audit response tasks, the ARC group allows healthcare providers to allocate more resources to core mission activities like patient care and innovation in healthcare delivery.

How Healthcare Providers Can Use ARC Services

- **Continuous Improvement:**
  - **Feedback Loop:** The ARC group proactively seeks feedback to improve processes and collaborates with healthcare providers to implement best practices, further enhancing efficiency and service delivery.
  - **Updated Policies:** Keeping healthcare providers informed of the latest regulatory updates and cybersecurity trends helps in maintaining compliance and being prepared for future audits.

- **Risk Mitigation:**
  - **Vulnerability Management:** By supporting POA&M activities, the ARC group helps in the timely identification and remediation of vulnerabilities, reducing the risk of data breaches and ensuring continuous operation.

In summary, the ARC group's comprehensive suite of services plays a vital role in simplifying compliance and audit response efforts for healthcare providers.

Risk and Compliance offerings for Healthcare Professionals, Including Healthcare Providers and Facility Managers

Elevating Healthcare Security – A Call to Action for Professionals:

Now we step into Risk and Compliance offerings and how we can collectively and collaboratively elevate the security and resilience of our healthcare infrastructure. In an era where technology and data are the lifeblood of healthcare, securing this lifeblood is not merely an option—it's a necessity.

- **The New Healthcare Paradigm:**
  - Increasing reliance on data and technology.
  - Rising threats and vulnerabilities.
  - The critical need for robust security measures.
- **The Stakes Are High – Why Security Matters:**
  - Statistics on recent healthcare data breaches.
  - Financial, reputational, and operational consequences.
  - The moral imperative to protect patient data.
- **Imagine a Secure Healthcare Environment:**
  - Proactive risk identification and mitigation.
  - Protection of sensitive patient data.
  - Seamless compliance with stringent regulations.

Risk and Compliance Offerings for Healthcare Professionals, Including Healthcare Providers and Facility Managers

- **Introducing the Risk and Compliance Team:**
  - Who we are and our mission.
  - Our expertise and independent assessment capabilities.
  - The value we bring to healthcare providers and facility managers.
- **Comprehensive Benefits for Healthcare Professionals:**
  - Enhanced Patient Safety and Care Quality.
  - Improved Data Security and Privacy.
  - Operational Efficiency and Cost Savings.
  - Increased Confidence and Trust.
  - Continuous Improvement and Readiness.
- **Practical Steps to Fortify Security and Compliance:**
  - Conducting risk assessments.
  - Implementing robust security controls.
  - Regular training and awareness programs.
  - Continuous monitoring and adaptation

Risk and Compliance Offerings for Healthcare Professionals, Including Healthcare Providers and Facility Managers

- **The Importance of NIST Guidelines:**
  - Overview of NIST guidelines and their importance.
  - Steps to adhere to NIST standards.
  - Real-world examples of successful implementation.
- **Real-Life Success Stories:**
  - Case studies of healthcare facilities that benefited from our services.
  - Testimonials from healthcare professionals.
  - Quantifiable improvements in security and compliance.
- **Your Role in This Mission:**
  - The critical role of Information Security Officers and System Owners.
  - How individual contributions lead to collective success.
  - Encouragement to take immediate, proactive steps.
- **Let's Forge Ahead Together:**
  - Reiterate the importance of this mission.
  - Extend an invitation to partner with the Risk and Compliance team.
  - Contact information and pathways to engage further.

Risk and Compliance Offerings for Healthcare Professionals, Including Healthcare Providers and Facility Managers

Closing Statement

With the dynamic nature of the healthcare landscape, every Information Security Officer and System Owner must take an assertive stance in protecting the sanctity of the information we handle. By diligently adhering to the NIST publication guidelines, you will, not only fortify our systems against potential threats, but also ensure the integrity, confidentiality, and availability of crucial patient data. Your proactive engagement in this endeavour empowers us to continue serving our nation with unwavering dedication, maintaining the trust bestowed upon us by those we care for. Let's take this vital step together, ensuring that our commitment to security and compliance translates into a higher standard of health and safety for all. Together, we can make a profound difference. Thank you.

Cybersecurity Policy and Security Awareness (PSA) Empower Your Healthcare Facility with DIS PSA Services

In the rapidly evolving healthcare industry, the need for robust cybersecurity policies and comprehensive security awareness programs is more critical than ever. Healthcare professionals and facility managers are responsible for not only protecting sensitive patient information but also ensuring that every employee and service provider is vigilant and knowledgeable about cybersecurity threats. The DIS Cybersecurity Policy and Security Awareness (PSA) team is dedicated to fostering a culture of security for overall all IHS user community. Aligned with risk governance protection standards described by the Department of Health and Human Services (HHS), the CISA, and NIST publications, our services aim to energize and enable your workforce. By developing and disseminating effective cybersecurity policies and conducting awareness programs, we ensure everyone in IHS is prepared to take all necessary actions to protect Healthcare information delivering the healthcare services securely.

Why Choose DIS PSA Services?

1

COMPREHENSIVE EXPERTISE

The DIS PSA team consists of professionals experienced in crafting and implementing cybersecurity policies and awareness programs specifically for the healthcare sector. Our expertise ensures that your policies are not only compliant with HHS, CISA, and NIST standards but also practical and effective

2

TAILORED TRAINING AND AWARENESS PROGRAMS

We provide customized training programs designed to meet the specific needs of your healthcare facility. Our security awareness initiatives are tailored to different roles within your organization, ensuring that everyone—from front-line staff to executive leadership—is knowledgeable and vigilant.

3

REGULATORY COMPLIANCE

Our policy development and awareness programs align with HHS guidelines, CISA recommendations, and NIST standards such as NIST SP 800-50 (Building an Information Technology Security Awareness and Training Program) and NIST SP 800-53 Rev. 5 (Security and Privacy Controls for Information Systems and Organizations). This alignment ensures your Healthcare services remains compliant with critical regulations and standards.

4

CULTURE OF SECURITY

We believe that cybersecurity is a collective responsibility. Our PSA services aim to foster a culture of security within your organization, encouraging proactive participation and vigilance from all employees and service providers

5

ONGOING SUPPORT AND IMPROVEMENT

Cybersecurity is an evolving field. We provide ongoing support to ensure that your policies and awareness programs remain up to date with the latest threats and best practices.

6

TRAINING AND AWARENESS PROGRAMS

Educate your staff on cybersecurity best practices and the importance of maintaining a secure environment. Our training programs are designed to foster a culture of security awareness and proactive defense

Key Services Offered by DIS PSA Team

- **Cybersecurity Policy Development:**
  - Create and update comprehensive cybersecurity policies that align with HHS, CISA, and NIST standards. Our policies cover various aspects of information security, from data protection and access controls to incident response and vendor management.
- **Security Awareness Training:**
  - Conduct regular training sessions tailored to different roles within your organization. Our interactive and engaging training programs cover essential topics such as phishing prevention, password management, data handling, and incident reporting.
- **Information Dissemination:**
  - Implement effective communication strategies to disseminate critical cybersecurity information throughout your organization. We use various channels, including newsletters, intranet portals, and town hall meetings, to ensure that everyone stays informed and vigilant
- **Incident Response Simulations:**
  - Conduct tabletop exercises and simulations to prepare your staff for potential cybersecurity incidents. These hands-on activities help employees understand their roles and responsibilities during an incident, ensuring a coordinated and effective response
- **Security Awareness Campaigns:**
  - Launch comprehensive awareness campaigns that promote cybersecurity best practices. Our campaigns include posters, emails, webinars, and workshops designed to keep cybersecurity top of mind for all employees and service providers.

Key Services Offered by DIS PSA Team

- **Compliance and Audit Support:**
  - Provide guidance and support to ensure your Healthcare services meets regulatory requirements and passes audits. We help document your cybersecurity policies and awareness programs, providing evidence of compliance with HHS, CISA, and NIST standards.
- **Continuous Monitoring and Feedback:**
  - Establish mechanisms for continuous monitoring of policy effectiveness and employee awareness. We gather feedback, conduct assessments, and implement improvements to ensure your cybersecurity posture remains strong.
- **Vendor and Provider Education:**
  - Extend security awareness and policy training to third-party vendors and service providers. Ensuring that all external partners are aligned with your cybersecurity standards is crucial for maintaining a secure ecosystem.
- **Phishing Exercises:**
  - Develop and conduct phishing exercises to educate employees about email-based threats. These exercises simulate real-world phishing attempts, helping staff recognize malicious emails and reinforcing the importance of vigilance in protecting both personal and agency data.
- **Training Development and Community Building:**
  - Launch comprehensive awareness campaigns that promote cybersecurity best practices. Our campaigns include posters, emails, webinars, and workshops designed to keep cybersecurity top of mind for all employees and service providers.

By Partnering with the DIS PSA Team, Your Healthcare Facility Can:

Enhance Security Culture

Create an environment where cybersecurity is a shared responsibility, promoting proactive participation and vigilance from all employees and service providers.

Protect Data and Reputation

Through regular phishing exercises and comprehensive training, ensure that all employees know how to protect not only their personal data but also the agency's data and reputation from cyber threats.

Ensure Regulatory Compliance

Maintain compliance with HHS, CISA, and NIST standards through well-crafted policies and comprehensive awareness programs, protecting your Healthcare services from legal liabilities.

Strengthen Organizational Resilience

Build a resilient organization equipped to handle cybersecurity challenges through ongoing training, simulations, and continuous improvement programs.

Reduce Cybersecurity Risks

Empower your staff with the knowledge and skills needed to recognize and respond to cybersecurity threats, reducing the risk of data breaches and other incidents.

Support Modernization Efforts

Foster a secure foundation for your health modernization initiatives, ensuring that new technologies are deployed safely and effectively.

By Partnering with the DIS PSA Team, Your Healthcare Facility Can:

In the high stakes world of healthcare, robust cybersecurity policies and awareness programs are essential for protecting sensitive data and ensuring smooth operations. The DIS Cybersecurity Policy and Security Awareness (PSA) team is here to provide you with the expertise, tools, and strategies needed to cultivate a security conscious workforce. Our comprehensive and tailored approach, aligned with HHS, CISA, and NIST standards, ensures that your healthcare services remains secure, compliant, and resilient.

Take the next step in empowering your facility's cybersecurity. Contact the DIS PSA team today to schedule a consultation and discover how our services can enhance your cybersecurity policies and awareness initiatives.

Services Offered by DIS PSA Team

- **Expertise and Experience:**
  - Our ISSO team is composed of seasoned professionals with extensive knowledge in cybersecurity operations, risk management, and compliance. Their expertise ensures that your Healthcare services is well-protected against a wide range of security threats.
- **Comprehensive Risk Management:**
  - Our ISSO services encompass all aspects of risk management, from identification and assessment to strategic mitigation. We help you manage and mitigate risks effectively, ensuring resilience against cyber threats.
- **Compliance Assurance:**
  - DIS ISSO services ensure compliance with federal and industry regulations. We manage the development and maintenance of ATO packages, guaranteeing that your Healthcare services meets stringent standards like NIST, HIPAA, and FISMA.
- **Proactive Threat and Vulnerability Management:**
  - Our ISSO team provides continuous monitoring and management of potential threats and vulnerabilities. Employing advanced tools and methodologies, we proactively address risks before they can impact your operations.
- **Dedicated Oversight:**
  - Having a dedicated ISSO ensures continuous prioritization and expert management of cybersecurity efforts across your organization. Our team provides strategic guidance and operational oversight to enhance your security posture.

- Open floor for participant questions
- Addressing specific concerns and clarifying concepts
- Interactive discussion to engage the audience

Conclusion

In the challenging landscape of healthcare cybersecurity, maintaining and managing efficient cybersecurity operations and risk management require dedicated expertise and strategic oversight. The DIS offers ISSO services that provide comprehensive management of cybersecurity operations, threats, vulnerabilities, and compliance. Our experienced professionals ensure your Healthcare services remains secure, compliant, and resilient.

THANK YOU

Take the next step in fortifying your cybersecurity posture. Contact the DIS team leads today to schedule a consultation and discover how our services can enhance your cybersecurity operations and risk management efforts.

Together, we can deliver secure healthcare.


INDIAN HEALTH SERVICE
PHS · 1955 ·