**Cyber Threats to Sensitive Content Communications**

Findings From Kiteworks’ 2023 Sensitive Content Communications Privacy and Compliance Report

- **Number of Sensitive Content Communication Exploits in the Past Year by Organization**
  - 10+ 13%
  - 7 - 9 23%
  - 4 - 6 48%
  - 2 - 3 15%
  - 1 1%

- **Regional Distribution**
  - NAM: 10+ 14%
  - Asia Pacific: 7 - 9 25%
  - Middle East: 4 - 6 46%
  - Europe: 2 - 3 16%

- Top Attack Vector Concerns for Sensitive Content Communications

- **Top Attack Vectors Per Region**
  - NAM: 1. Password/Credential Attacks
  - Asia Pacific: 1. Password/Credential Attacks
  - Middle East: 1. Password/Credential Attacks

- **Weighed Algorithmic Score**
  - Password/Credential Attacks: 63
  - DNS Tunneling: 66
  - Denial of Service: 70
  - URL Manipulation: 60
  - Cross-site Scripting: 64
  - Rootkits: 29

- **Top 3 Attack Vectors Per Industry**
  - Energy and Utilities: 1. Password/Credential Attacks
  - Federal Government: 1. Session Hijacking
  - Financial Services: 1. URL Manipulation
  - Healthcare: 1. Password/Credential Attacks
  - Higher Education: 1. Password/Credential Attacks
  - Legal/Law Firms: 1. Rootkits
  - State Government: 1. DNS Tunneling
  - Local Government: 1. Denial of Service
  - Manufacturing: 1. Phishing
  - Pharmaceutical/Life Sciences: 1. Rootkits
  - Professional Services: 1. DNS Tunneling
  - Security/Defense: 1. Password/Credential Attacks
  - Technology: 1. DNS Tunneling

- **Largest Impact of an Exploit Across Regions**
  - Financial Implications: NAM 69%
  - Brand Impact: Europe 49.5%
  - Compliance Penalties: Middle East 59%
  - IT 21.5%
  - Security 38%
  - Risk/Compliance 40%

- **For the entire 2023 Sensitive Content Communications Privacy and Compliance Report, click here.**