Stay Ahead of Cyber Threats

Fortifying Agencies Against Increasing Fraud Risk

Cybersecurity and Risk Management

This infographic series focuses on several of **National Association of State Chief Information Officers' (NASCIO's)[1] top priority pillars**, which identify and prioritize the biggest policy and technology issues facing government agencies – and provides possible solutions for addressing these needs. The last in our series is **Cybersecurity and Risk Management**.

Cybersecurity threats are evolving faster than defenses, and the public sector is under immense pressure to keep up. Threats like ransomware, phishing, and state-sponsored attacks are becoming more sophisticated, and with budget constraints limiting security measures, public sector entities are at heightened risk.

Holding the Data Captive with Ransomware

Ransomware remains one of the most dangerous cyber threats, targeting critical public sector systems. Beyond encrypting data, critical information systems can be taken offline while hackers employ double extortion by threatening to publicly post sensitive citizen information if ransom demands are not met. For government agencies hosting state and federal essential infrastructure, the stakes are higher than ever.

The average ransom payment in 2024 has risen to $2.73 million, nearly a $1 million increase from 2023.[2]

The most common tactics hackers use to carry out ransomware attacks are email phishing campaigns, Remote Desktop Protocol (RDP) vulnerabilities, and software vulnerabilities.[3]

State-Sponsored Cyberattacks

State-sponsored cyberattacks have surged dramatically due to rising geopolitical tensions. Unlike financially motivated cyberattacks, state-sponsored operations aim to disrupt essential services and compromise security on a geopolitical scale. These attacks are typically conducted to achieve strategic or political objectives, such as:

Espionage: Stealing sensitive information, like intellectual property or state secrets, to gain an advantage in international relations, economics, or military affairs.

Sabotage: Disrupting or damaging critical infrastructure, such as power grids, financial systems, or communication networks, to destabilize an opponent or weaken its national security.

Influence Operations: Disrupting elections, spreading disinformation, or manipulating public opinion to influence political outcomes in favor of the sponsoring state.

Economic Warfare: Attacking financial systems, industries, or commerce to harm the economy of the target nation.

The path of least resistance into government agencies is compromised credentials.

58% of nation-state cyberattacks come from and 79% of nation-state attackers target government agencies, non-government organizations (NGOs), and think tanks.[4]

In 2023, the United States experienced over 420 million attacks on critical infrastructure, averaging 13 attacks per second.[5]

Phishing, Smishing, and Quishing Schemes

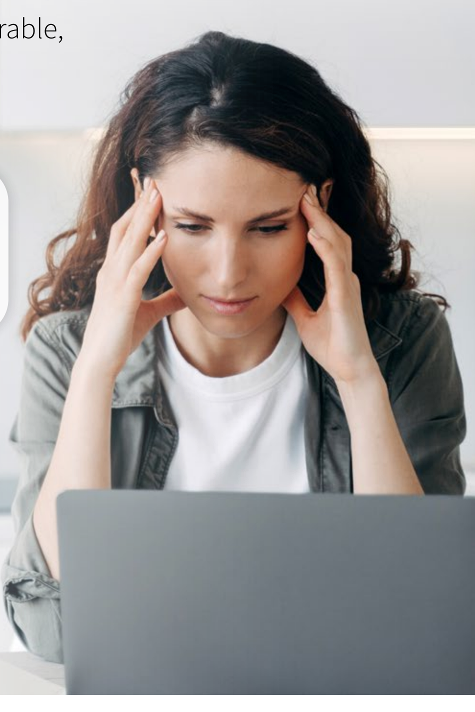
Despite growing awareness, phishing, smishing, and quishing remain serious vulnerabilities for government agencies and those they serve. These socially engineered attacks exploit human emotions to mistakenly trust a message, often tricking employees into exposing sensitive information. For public sector organizations, such breaches can lead to compromised citizen data, identity theft, and disruption of critical services. Government information systems with weak authentication are especially vulnerable.

In the third quarter of 2024, the Anti-Phishing Working Group (APWG) reported 932,923 phishing attacks, a rise from 877,536 in the previous quarter.[6]

QR code phishing ("quishing") has surged, with QR codes being used in 22% of all phishing attacks in 2023.[7]

Disaster Strikes with Distributed Denial of Service (DDoS)

DDoS attacks threaten to overwhelm government servers, denying access to websites and services citizens rely on every day. Such disruptions create public confusion, damage trust, and destabilize essential operations. Beyond immediate service disruptions, DDoS attacks can have broader implications – by diverting information technology resources to mitigate these attacks, agencies may become more susceptible to other cyber threats, such as data breaches or malware infiltrations. The financial burden associated with countering DDoS attacks is also considerable, encompassing costs related to system restoration, implementation of enhanced security measures, and potential legal liabilities.



In the first half of 2024, DDoS attacks globally increased by 102% compared to the same period in 2023. The government sector was the hardest hit, experiencing a 116% year-on-year increase, accounting for 29% of all DDoS incidents.[8]

In the fourth quarter of 2023, the government sector experienced a significant surge in Distributed Denial of Service (DDoS) attacks, accounting for 66% of the 1,000 largest attacks mitigated by Lumen® Technologies. This marked a 163% increase from the previous quarter and a staggering 4,025% rise compared to the same period the previous year.[9]

Outdated Infrastructure Roadblocks

Outdated technology infrastructure can significantly hinder the efficiency and effectiveness of government agencies. Legacy systems, often built decades ago, may struggle to integrate with modern technologies, leading to fragmented operations and data silos. These inefficiencies can slow critical processes and create technical failures, downtime, and cyber vulnerabilities. For government agencies tasked with serving the public, such limitations can result in delays, errors, and diminished trust from constituents who expect timely and accurate services.

A report by the Center for Internet Security (CIS) indicates that all types of cyberattacks against state and local governments rose in 2023. This surge is attributed to various factors, including the reliance on outdated systems that are no longer supported or easily patched against new cyber threats.[10]

A June 2024 report from the Cyber Threat Intelligence Integration Center (CTIIC) highlights that outdated software, poor password security, and the use of default credentials have rendered critical U.S. government services susceptible to cyberattacks.[11]

Human Error: Mistakes Happen

Even with robust security in place, human error remains a significant security risk. Employees in government roles often handle classified data, personal information, and critical infrastructure systems, potentially making mistakes such as weak password management, falling victim to phishing schemes, or misconfiguring IT systems. For example, a single instance of clicking on a malicious link in a phishing email can grant attackers access to an agency's network, potentially exposing confidential records or disrupting vital operations.

A 2024 report by Varonis indicates that 88% of cybersecurity breaches are caused by human error.[12]

A 2024 survey found that 66% of Chief Information Security Officers (CISOs) in the United States consider human error their organization's top cybersecurity vulnerability.[13]

Risk Management Matters

Risk management is critical for government agencies to protect both their operations and the people they serve from the growing threat of cyberattacks. With the increasing reliance on digital technologies and the interconnectedness of systems, government agencies are prime targets for malicious actors seeking to exploit vulnerabilities. **A well-structured risk management strategy helps agencies identify, assess, and mitigate potential threats before they can cause significant harm.** By proactively addressing risks, agencies can ensure:

- **Continuity of critical services**
- **Safeguard sensitive data**
- **Maintain public trust**

This is particularly important as cyberattacks on government infrastructure can disrupt essential services, undermine national security, and compromise the privacy of citizens.

Effective risk management also empowers government agencies to stay ahead of emerging cyber threats. Cybercriminals are constantly evolving their tactics, and without a robust framework for monitoring and responding to risks, agencies may find themselves ill-prepared for new challenges. Agencies can adapt to the rapidly changing threat landscape by regularly:

- **Updating security protocols**
- **Conducting vulnerability assessments**
- **Implementing incident response plans**

Discover the Solution to Combat Cyber Threats

It takes a network to break a network. LexisNexis® Risk Solutions helps government agencies improve their overall cybersecurity posture by offering **enhanced identity threat intelligence** as well as **identity and device risk assessment capabilities**.

Experience the Power of LexisNexis EssentialID™

- **Address Identity Workflow Vulnerabilities**
- **Prioritize Identity-related Cybersecurity Initiatives**
- **Deploy Resources More Effectively**

LexisNexis EssentialID™ is an award-winning, seamless, and secure identity orchestration platform providing multi-layered, fraud-resistant identity verification, third-party data integration and decision-making capabilities. EssentialID™ empowers government entities to respond swiftly to identity-related cyber threats, avoid damage to the agency, and strengthen resilience against future attacks.

LexisNexis EssentialID™ helps agencies outsmart cyber threats before they start.

LexisNexis® RISK SOLUTIONS

Find out more about the power of LexisNexis EssentialID™. Scan the QR code or call us at 1.888.216.3544.

1. https://www.nascio.org/resource-center/resources/state-cio-top-ten-policy-and-technology-priorities-for-2024/
2. https://www.varonis.com/blog/ransomware-statistics
3. https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf
4. https://www.varonis.com/blog/cybersecurity-statistics
5. https://www.huntress.com/blog/which-states-are-most-at-risk-for-cyberattacks-on-government-and-infrastructure?utm_source=chatgpt.com
6. https://apwg.org/trendsreports/
7. https://keepnetlabs.com/blog/2024-qr-code-phishing-trends-in-depth-analysis-of-risin-quishing-statistics
8. https://www.infosecurity-magazine.com/news/ddos-attacks-double-govt-targeted/?utm_source=chatgpt.com
9. https://news.lumen.com/2024-02-08-Government-Sector-is-Top-Targeted-Industry-for-DDoS-Attacks-in-Q4-2023?utm_source=chatgpt.com
10. https://statescoop.com/ransomware-malware-cyberattacks-cis-report-2024/?utm_source=chatgpt.com
11. https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf?utm_source=chatgpt.com
12. https://www.varonis.com/blog/cybersecurity-statistics?utm_source=chatgpt.com
13. https://www.statista.com/statistics/1448350/ciso-human-error-organization-cyber-vulnerability-global/?utm_source=chatgpt.com

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.