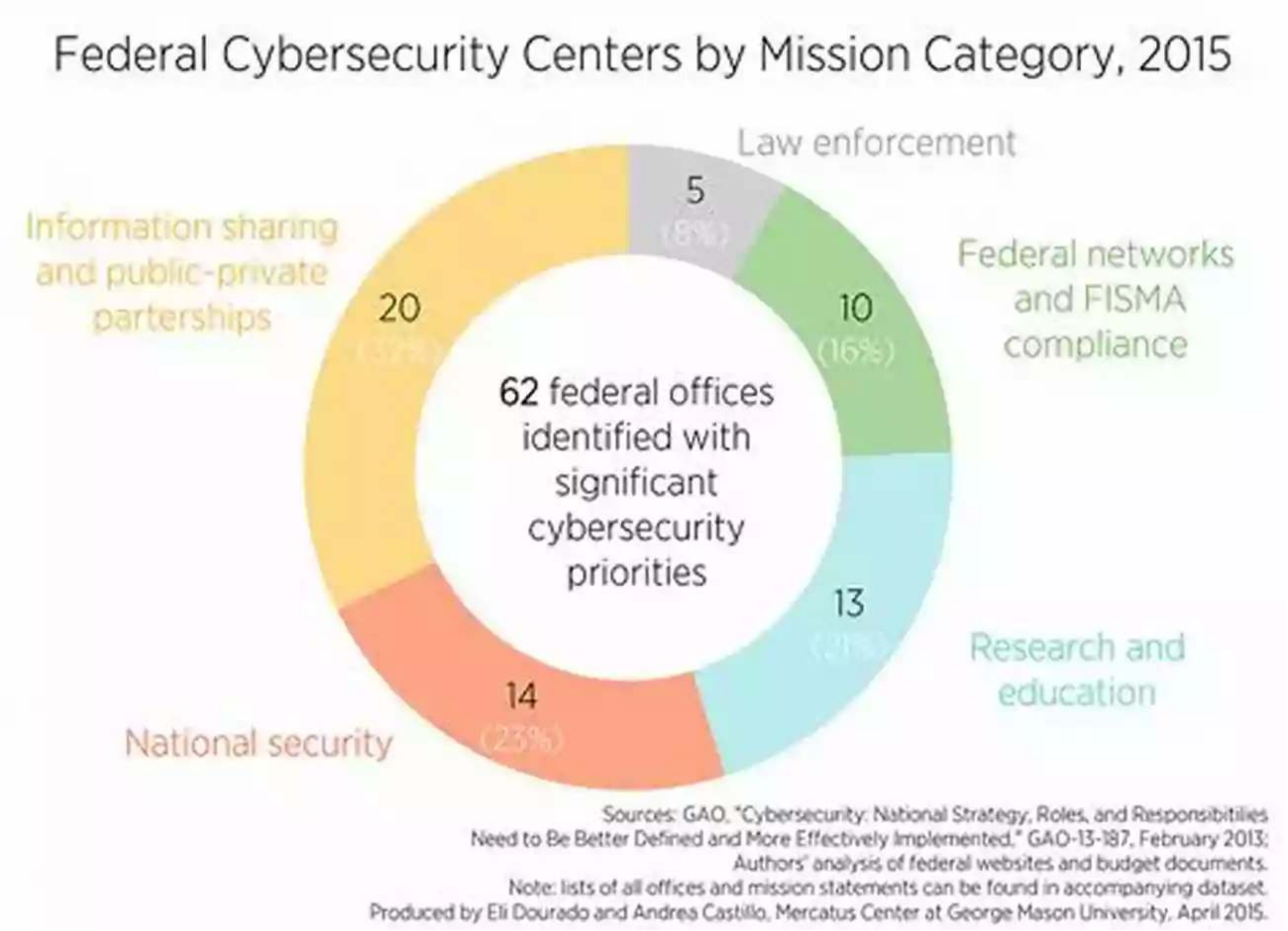
Is America's Data at Risk? Federal Cybersecurity Under Scrutiny



Federal Cybersecurity Centers by Mission Category, 2015

Sources: GAO, "Cybersecurity: National Strategy, Roles, and Responsibitilies Need to Be Better Defined and More Effectively Implemented," GAO-13-187, February 2013; Authors' analysis of federal websites and budget documents.
Note: lists of all offices and mission statements can be found in accompanying dataset.
Produced by Eli Dourado and Andrea Castillo, Mercatus Center at George Mason University, April 2015.

In today's interconnected world, data has become one of the most valuable assets for individuals, organizations, and nations alike. The United States, being a global leader in technology and innovation, possesses an extensive amount of sensitive data that is at constant risk from cyber threats. From government agencies to critical infrastructure, the nation's cybersecurity measures are paramount to ensure the protection and integrity of data.

The Evolving Threat Landscape

As technology advances and cybercriminals become more sophisticated, the threat landscape has undergone a significant transformation. Hackers, both state-sponsored and individual actors, target critical infrastructure, government systems, and private entities to breach data and wreak havoc. The motive behind these attacks could range from financial gain to gathering sensitive intelligence or disrupting essential services.

United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs

FEDERAL CYBERSECURITY:
AMERICA'S DATA AT RISK

STAFF REPORT

PERMANENT SUBCOMMITTEE ON
INVESTIGATIONS

UNITED STATES SENATE

Federal Cybersecurity: America’s Data At Risk

by David Roy Newby(Kindle Edition)

★★★★☆ 4.1 out of 5

Language	: English
File size	: 685 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Word Wise	: Enabled
Print length	: 250 pages
Lending	: Enabled

FREE DOWNLOAD E-BOOK PDF

The urgency to bolster the nation's cybersecurity measures has never been greater. The rapid adoption of advanced technologies like artificial intelligence, Internet of Things (IoT),and cloud computing has expanded the attack surface, providing more opportunities for cyber threats to exploit vulnerabilities.

Federal Government's Role in Cybersecurity

The federal government plays a vital role in safeguarding the nation's data and infrastructure from cyber threats. Agencies such as the Department of Homeland Security (DHS),National Security Agency (NSA),and Cybersecurity and

Infrastructure Security Agency (CISA) work together to establish and enforce cybersecurity policies, conduct threat intelligence, and respond to incidents.

The Federal Information Security Modernization Act (FISMA) and the Cybersecurity Enhancement Act provide a framework for federal agencies to strengthen their cybersecurity posture. The implementation of these acts ensures that agencies regularly assess risks, develop mitigation strategies, and report any incidents promptly. However, the evolving threat landscape demands continuous collaboration, innovation, and investment to counter emerging cyber threats.

America's Critical Infrastructure in the Crosshairs

The protection of critical infrastructure, such as power grids, transportation systems, and financial institutions, is an essential part of national security. The increasing connectivity of these systems poses a significant challenge as any disruption can have severe consequences on the economy, public safety, and daily life.

Cybersecurity vulnerabilities in critical infrastructure were evident during the 2015 Ukraine power grid attack and the recent ransomware attack on the Colonial Pipeline. These incidents highlight the need for robust security measures to protect against cyber threats that can potentially paralyze critical infrastructure and cause widespread disruption.

Securing the Government's Digital Domain

Government agencies house a vast amount of sensitive data, including classified information, personally identifiable information (PII),and intellectual property. The protection of such data is crucial for preserving national security, upholding privacy rights of citizens, and maintaining trust in government institutions.

While federal agencies have made significant strides in improving their cybersecurity posture, high-profile breaches like the Office of Personnel Management (OPM) hack in 2015 have raised concerns about the effectiveness of existing measures. Continuous efforts to enhance workforce training, modernize legacy systems, establish real-time threat intelligence sharing, and implement robust identity management protocols are essential to tackle these challenges.

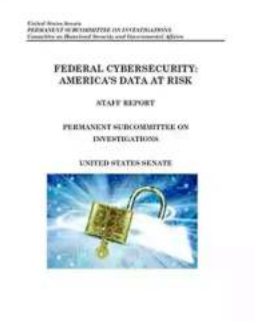
The Role of Public-Private Collaboration

Cybersecurity is not solely the responsibility of the federal government; it requires the active participation and collaboration of the private sector as well. Many critical infrastructures and key industries are owned and operated by private entities, making their involvement critical in defending against cyber threats.

The sharing of threat intelligence, best practices, and expertise between the government and private sector can significantly strengthen the nation's cybersecurity posture. Collaborative efforts, such as the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) program, aim to ensure adequate security controls and practices are implemented by contractors working with sensitive government data.

The United States faces an ever-increasing cyber threat landscape that puts the nation's data, critical infrastructure, and overall security at risk. By recognizing the evolving nature of cyber threats and adapting to emerging challenges, the federal government can play a significant role in securing America's digital domain.

Collaboration between public and private entities, continuous investment in cybersecurity measures, and the pursuit of innovative solutions can help mitigate risks and protect the nation's sensitive data. Harnessing the power of technology and human ingenuity, America can overcome the challenges of the digital era and ensure a safer, more secure future for all.



FEDERAL CYBERSECURITY: AMERICA'S DATA AT RISK

STAFF REPORT

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

Federal Cybersecurity: America’s Data At Risk

by David Roy Newby(Kindle Edition)

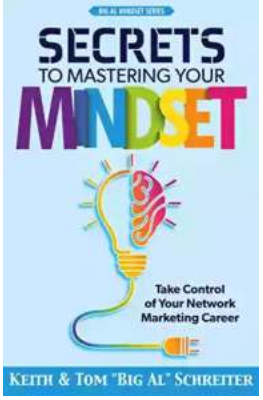
★★★★☆ 4.1 out of 5

Language	: English
File size	: 685 KB
Text-to-Speech	: Enabled
Screen Reader	: Supported
Enhanced typesetting	: Enabled
Word Wise	: Enabled
Print length	: 250 pages
Lending	: Enabled

Federal government agencies are the frequent target of cybersecurity attacks. From 2006 to 2015, the number of cyber incidents reported by federal agencies increased by more than 1,300 percent. In 2017 alone, federal agencies reported 35,277 cyber incidents. The Government Accountability Office (“GAO”) has included cybersecurity on its “high risk” list every year since 1997.

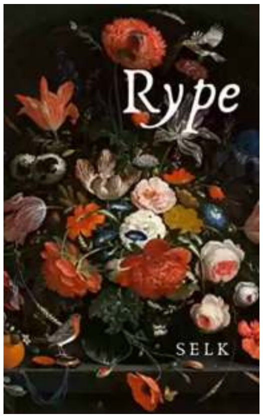
No agency is immune to attack and the list of federal agencies compromised by hackers continues to grow. In the past five years, agencies reporting data breaches include the United States Postal Service, the Internal Revenue Service, and even the White House. One of the largest breaches of government information occurred in 2015 when a hacker ex-filtrated over 22 million security clearance files from the Office of Personnel Management (“OPM”). Those files contained extensive personal and potentially comprising information. We may never know the full impact on our national security of the OPM breach.

The number of data breaches agencies have reported in recent years is not surprising given the current cybersecurity posture of the federal government. A recent report by the Office of Management and Budget ("OMB") made clear that agencies "do not understand and do not have the resources to combat the current threat environment." This is especially concerning given the information agencies must collect and hold. This report documents the extent to which the federal government is the target of cybersecurity attacks, how key federal agencies have failed to address vulnerabilities in their IT infrastructure, and how these failures have left America's sensitive personal information unsafe and vulnerable to theft.



Take Control Of Your Network Marketing Career

Are you tired of working long hours to build someone else's dream? Do you dream of escaping the monotonous 9-to-5 job and achieving financial freedom? ...



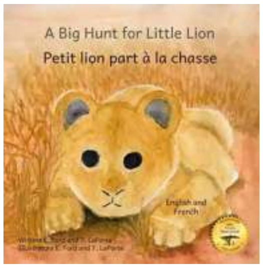
The Enigmatic Talent of Rype Jen Selk: A Musical Journey Like No Other

When it comes to musical prodigies, there are few that can match the enigmatic talent of Rype Jen Selk. With a musical journey that spans across genres and ignites a...

Journal of Shi'a Islamic Studies
Winter 2013 · Volume VI · Number 1
Islamic College, London, UK

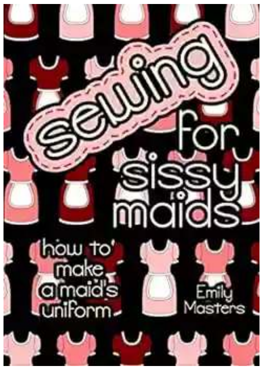
Unveiling the Rich History and Poetry of Shiraz in Iranian Studies 10

When it comes to the cultural heritage of Iran, few cities can rival the richness and significance of Shiraz. Known as the City of Love and Poetry, Shiraz has...



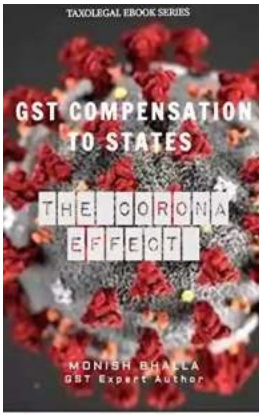
How Impatience Can Be Painful In French And English

: In today's fast-paced world, impatience has become an ever-present aspect of our lives. We are constantly seeking instant gratification, wanting things to happen quickly...



Sewing For Sissy Maids - Unleashing Your Creative Side

Are you ready to dive into the enchanting world of sewing for sissy maids? Whether you want to create your own beautiful sissy maid outfits or indulge in...



GST Compensation to States: Ensuring Fiscal Stability during the Pandemic

In the wake of the COVID-19 pandemic, governments around the world have been grappling with the economic fallout, trying to find ways to stabilize their economies and...

HOW TO PLAY
BLACKJACK
Guide On How To Play Blackjack For Beginners, The Strategy, Rules, Instructions And Winning Tips
MARCEL PEART

Learn How to Play Blackjack: A Comprehensive Guide for Beginners

Blackjack, also known as twenty-one, is one of the most popular card games in both brick-and-mortar and online casinos. This thrilling game of skill and luck has been...

THE BELGIAN TRAVELLER: A COMPLETE GUIDE THROUGH BELGIUM AND HOLLAND, OR KINGDOMS OF THE UNITED NETHERLANDS. WITH A SKETCH OF THE HISTORY, CONSTITUTION, AND RELIGION OF THE NETHERLANDS, ETC
EDMUND BOYCE

Complete Guide Through Belgium And Holland Or Kingdoms Of The United

Welcome, travel enthusiasts, to a complete guide through Belgium and Holland - the enchanting Kingdoms of the United! This picturesque region offers a delightful...