John D. Williams

Baylor University

ISEC 5405 Cybersecurity Fundamentals

Prof: Nicholas Simmons

11/26/2023

CYBERSECURITY THREAT LANDSCAPE: A GOVERNMENT SECTOR ASSESSMENT

An Executive Summary of Breach Impacts and Risk Management

Purpose and Problem

In an era where information is as vital as infrastructure, safeguarding our government's data is not just a policy matter but the bedrock of public faith. This executive summary delves into the web of cyber threats that shadow government operations at all levels. I illuminate the pressing challenges and the strategy necessary for bolstering cybersecurity defenses through an examination of recent breaches.

The consequences of cybercrime are profound, impacting not just the fiscal ledger but the integrity of public service. The urgency for a fortified cyber defense is apparent with the fiscal losses due to cyber incidents in the United States topping $3.5 billion in as reported by the FBI in 2019. My analysis, anchored in data from the Privacy Rights Clearinghouse complemented by my insights, maps out the threat landscape the government sector has found themselves navigating.

The incidents we dissect here, though only a fraction of the broader narrative, signal a troubling rise in both the sophistication and frequency of cyberattacks. These case studies are the impetus for a broader conversation on risk management and developing resilient information security frameworks. In line with the NIST 800-30 principles, my assessment is designed to enhance the cyber fortitude of governmental infrastructures in the face of ever-evolving digital threats.

Adopting a Threat-Oriented Analysis Approach, we recognize the intent and capability of adversaries. This approach allows us to advise on proactive countermeasures, hypothetically providing leadership with the actionable intelligence needed to make strategic cybersecurity investments.

With that, the stage is set for a detailed Risk Assessment Report, offering a foundational understanding of the critical nature of cybersecurity within the government sector. It is a clarion call for decisive and informed action to defend the public sphere from the cyber dangers that threaten service continuity and the cornerstone of public confidence.

"FBI Releases the Internet Crime Complaint Center 2019 Internet Crime Report." Federal Bureau of Investigation, 2019, https://www.fbi.gov/news/press-releases/fbi-releases-the-internet-crime-complaint-center-2019-internet-crime-report.

Risk Assessment Method

The following is my roadmap to a successful study of the risks the American government has faced in the past to accurately predict what challenges will come.

TASK 1-1: IDENTIFY PURPOSE

This risk assessment is dedicated to dissecting the landscape of cyber threats that loom over government entities. The intent is to dissect the potential impact of these dangers on the operational integrity of government bodies, the confidentiality of citizen data, and the overarching trust in public institutions. It is this understanding that will drive cybersecurity defenses and the resilience of our national institutions.

TASK 1-2: IDENTIFY SCOPE

My investigation spans three unique areas of the government sector, cutting across the federal to the local levels. The timeline of this scrutiny is set against the backdrop of the most recent and relevant cyber events, providing an acute assessment of the present-day digital risk landscape.

TASK 1-3: IDENTIFY ASSUMPTIONS AND CONSTRAINTS

The assessment assumes that government entities are high-value targets for cyber adversaries due to the sensitive nature of the data they hold. My analysis is conducted within the bounds of classified data restrictions, the fluidity of the cyber threat environment, and the varied cyber defense readiness across government agencies.

TASK 1-4: IDENTIFY INFORMATION SOURCES

My insights are drawn from PRC data made available to me during this course and the NIST guide. Public data from the FBI was also incorporated.

TASK 1-5: IDENTIFY RISK MODEL AND ANALYTIC APPROACH

My methodology is rooted in the NIST's guidelines, balancing qualitative discernment with quantitative precision. The approach is twofold: an acute analysis of current government HACK cases and a retrospective examination of historical breaches. This dual perspective informs my recommendations.

Case Study

Governments operate in a digital world under constant threat from cyber-attacks that can undermine national security and shake public confidence. Conducting a Cyber Risk Assessment is critical to preempt such attacks from the local governance. This is exemplified by cases from the City of Hesperia, California, Marines Memorial Association and Foundation, extending to the complexities of third-party contractors like J.B. Hunt Transport Inc.

City of Herperia Breach Summary

Incident Overview:
The City of Hesperia, CA, was subjected to a sophisticated cybersecurity breach on November 28, 2021, which was reported on February 7, 2022. Immediate action triggered an internal investigation, which concluded on January 7, 2022, identifying potential unauthorized access to personal information.

Threat-Oriented Analysis:

- Threat Sources: The advanced nature of the breach suggests the involvement of a competent actor, potentially with state-sponsored resources, focused on extracting sensitive resident information.
- Threat Events: The specifics of the breach tactics remain undisclosed, but indicators suggest the exploitation of network vulnerabilities or sophisticated social engineering tactics.
- Vulnerabilities: A discernible lack of cybersecurity resources points to significant vulnerabilities in the City's digital infrastructure, heightening its attractiveness to cyber adversaries.
- Likelihood: The sophistication and methodical execution of the breach signal a high likelihood of recurring incidents unless cybersecurity measures are substantially improved.
- Impact: The breach, involving residents' sensitive personal information, has profound implications for privacy and the erosion of public trust in local governance.
- Risk: This breach represents a severe risk to the City of Hesperia. It underscores the critical need for a fortified cybersecurity framework to defend against advanced and evolving cyber threats.

Response:
The City's response to the breach included immediate investigation, collaboration with law enforcement, and notification to the affected individuals. The City has taken measures to bolster cybersecurity defenses and has offered services such as credit monitoring and identity theft protection to mitigate potential harm to residents' financial security.

"Data Breach Reports." Office of the Attorney General, State of California Department of Justice, oag.ca.gov/ecrime/databreach/reports/sb24-550752. Accessed 11/26/2023.

Marines Memorial Association and Foundation Breach Summary

Incident Overview:
A cybersecurity breach at the Marines Memorial Association and Foundation on May 20, 2020, resulted in unauthorized access and compromised sensitive personal details, including Social Security numbers, of 2,822 individuals.

Threat-Oriented Analysis:

- Threat Sources: Threat occurred at Blackbaud a third party that holds Military record by an unknown actor.
- Threat Events: The incident involved a ransomware attack.
- Vulnerabilities: The breach signifies vulnerabilities within the organization's cybersecurity measures, notably protecting susceptible veteran data.
- Likelihood: Such sensitive data heightens the likelihood of targeted attacks, necessitating stringent security measures.
- Impact: The breach directly impacts the military community's security and could have far-reaching effects on national security, given the nature of the data involved.
- Risk: This incident denotes a significant risk, not just in terms of data exposure but also regarding the potential erosion of trust within the military community and beyond.

Response:
The Foundation's immediate offer of credit monitoring and identity theft protection services to affected individuals indicates a proactive stance on remediation. The rapid implementation of enhanced data security practices further reflects a commitment to bolstering the organization's cybersecurity infrastructure. The heightened national security concerns necessitate reviewing and reinforcing cybersecurity protocols within military-affiliated organizations.
This breach emphasizes the need for comprehensive cybersecurity strategies that preemptively address vulnerabilities. Efforts to restore confidence and support service members and veterans through transparent communication are the clear first step.

"Data Breaches." Privacy Rights Clearinghouse, privacyrights.org/data-breaches. Accessed 11/26/2023.

J.B. Hunt Transport Inc. Breach Summary

Incident Overview:
J.B. Hunt Transport Inc., serving as a government contractor, experienced a significant breach caused by a configuration error in a Microsoft Power Apps portal on October 20, 2021, in Iowa. This misconfiguration risked exposing sensitive personal data, including names and Social Security numbers of 2,063 individuals.

Threat-Oriented Analysis:

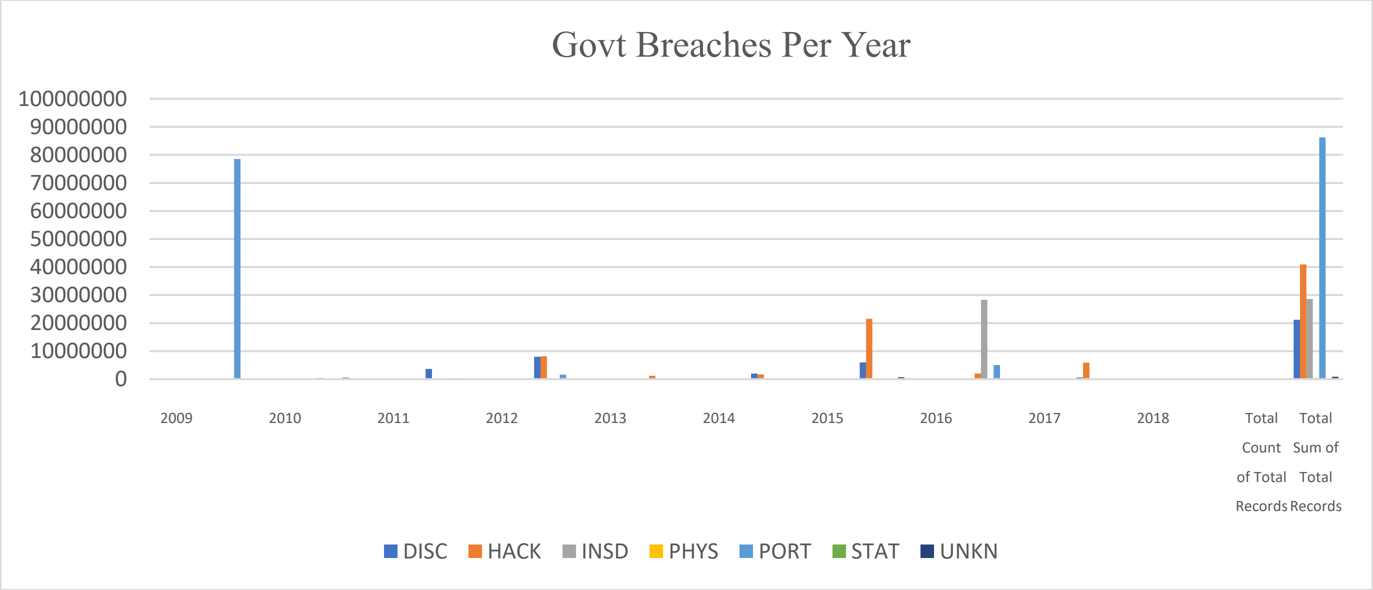
- Threat Sources: The breach resulted from internal misconfigurations rather than an external attack, highlighting issues within operational security practices.
- Threat Events: The misconfiguration event came from internal threats that can lead to significant data exposure.
- Vulnerabilities: The incident reveals vulnerabilities in implementing and managing cloud services, emphasizing the need for rigorous configuration controls
- Likelihood: The prolonged period before detection indicates a heightened likelihood of similar undetected vulnerabilities within cloud-based systems.
- Impact: The exposure of personal data carries the risk of identity theft and potential exploitation, substantially impacting affected individuals.
- Risk: The breach represents a considerable risk regarding data privacy and the integrity of sensitive information managed by third-party contractors.

Response:
J.B. Hunt Transport Inc.'s response involved immediate rectification measures to secure the portal, revise permission settings, and enhance cloud configurations. Providing credit monitoring services for those affected demonstrates a responsible approach to breach management. The breach underscores the critical importance of third-party contractor roles in government cybersecurity and the ripple effects their security posture can have. It accentuates the need for strict compliance measures, continuous technical training, and proactive data management strategies to prevent such occurrences.

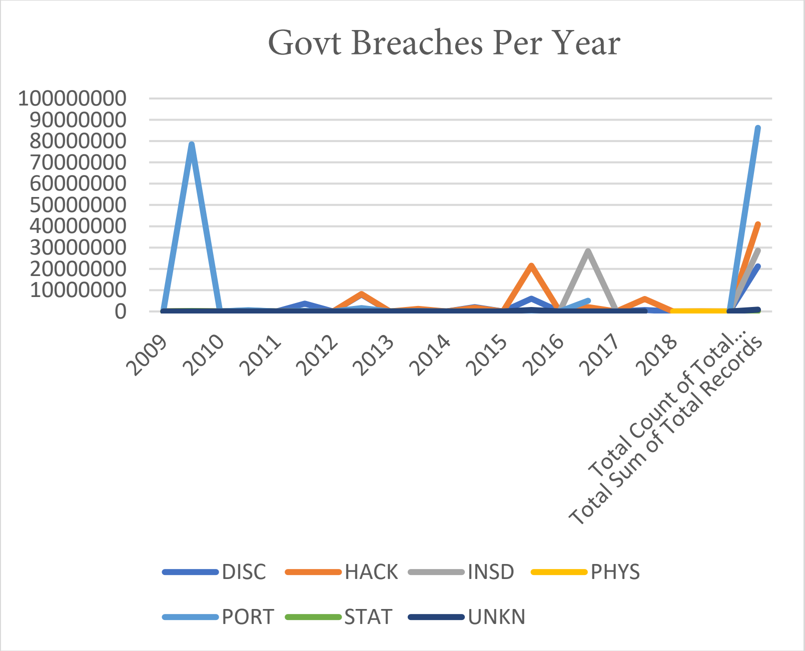
"Data Breaches." Privacy Rights Clearinghouse, privacyrights.org/data-breaches. Accessed 11/26/2023.

These three case studies highlight various weaknesses that could critically damage public trust and national security. Cyber threats are agnostic to an organization's prominence or scale, targeting vulnerabilities wherever they lie.

Results and Reccomendations



Analysis of GOVT breaches from 2009 to 2018 indicates an erratic yet notably increasing trend in cybersecurity incidents, particularly those categorized as hacking, which denotes a significant rise in both occurrences and the volume of records compromised. The disclosed data breaches experienced a pronounced peak in 2011, but the general trend has since shown a decline, which may reflect improved data handling protocols. However, the surge in insider breaches in 2016 raises critical concerns about the internal security of organizations and the need for stringent access controls.



Physical breaches have remained relatively constant and low in comparison, suggesting a possible shift in threat focus towards more technologically advanced methods of data compromise. Portable device breaches highlight significant episodic security lapses, emphasizing the ongoing challenge of securing mobile data.

This paper concludes that the integrity of public data and trust in government institutions hinges on a dynamic, informed, and strategic approach to cybersecurity. Government entities must champion this cause, ensuring the shield guarding our collective digital welfare remains unbreeched and steadfast.