Kevin C. Desouza and Kena Fedorschak | February 3, 2015 7:30am

The Vast Majority of the Government Lacks Clear Cybersecurity Plans

Cybersecurity

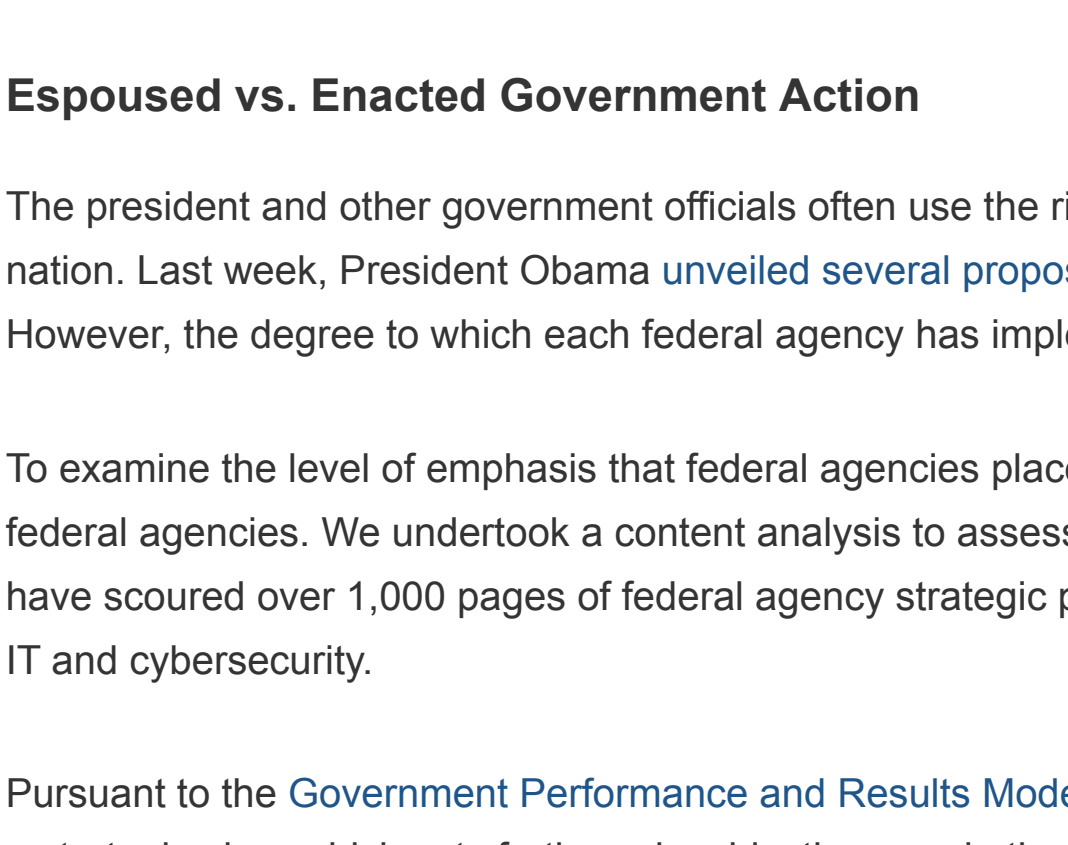
The public and private sectors use information technology (IT) every day to monitor, manage, and simplify their daily operations. The omnipresence of these technologies has introduced new vulnerabilities. Intelligence agencies, hackers, and other digital vandals can exploit security lapses and inflict extraordinary damage. The recent hacking of Sony Corporation, exposed authentication credentials for various internal systems, financial records, and private employee data including social security numbers and health records. Moreover, revelations that Sony's IT director previously served as a marketing executive and stored confidential information in plaintext demonstrates a flagrant disregard for cybersecurity.

Cyber Threat Proliferation

Cyberattacks have increased dramatically in recent years. Last January, Target opened the year by announcing that hackers gained access to 40 million credit and debit card numbers. In August, J.P. Morgan Chase announced a breach that affected an estimated 76 million households. In September, Home Depot disclosed a payment system breach affecting 53 million individuals.

These prodigious hacks have impacted government entities as well. According the GAO, the number of cyber threats to federal agencies increased by 782 percent between 2006 and 2012. The recent hacking of the U.S. military's Central Command Twitter account by the militant group ISIS is the most recent reminder of government vulnerability to cyber threats. Additionally, the Center for Strategic and International Studies has estimated the likely annual cost of cybercrime at over $400 billion. These figures underscore the importance of increased cybersecurity investments.

US Central Command Twitter Hacked by ISIS



Source: Twitter.com

Espoused vs. Enacted Government Action

The president and other government officials often use the right rhetoric when describing the cyberthreats facing the nation. Last week, President Obama unveiled several proposals designed to bolster U.S. cybersecurity laws. However, the degree to which each federal agency has implemented cybersecurity initiatives remains unclear.

To examine the level of emphasis that federal agencies place on cybersecurity, we studied the strategic plans of U.S. federal agencies. We undertook a content analysis to assess the scope of their cybersecurity-related IT initiatives. We have scoured over 1,000 pages of federal agency strategic plans to determine which agencies invest most heavily in IT and cybersecurity.

Pursuant to the Government Performance and Results Modernization Act of 2010, each federal agency must prepare a strategic plan, which sets forth goals, objectives, and other performance priorities. On average, each agency's plan is 65 pages, defines 5 overarching organizational goals, and includes a list of about 3 objectives describing specific strategies necessary to accomplish each goal. The Department of Health and Human Services' plan has perhaps the most details with 5 goals and 25 objectives delineated across 125 pages. The Department of Energy's plan includes relatively fewer details in a 32 page document with 3 goals and 12 objectives.

Federal Cybersecurity Plans

We found that approximately 35 percent of objectives contained some IT elements and about 12 percent of objectives were almost entirely IT initiatives. The Department of Agriculture, Department of Commerce, and Department of Health and Human Services emphasize IT the most, while the Department of State, Department of the Interior, and Department of the Treasury seem least interested in IT initiatives.

In studying the IT initiatives described in these plans, we find that the focus on cybersecurity is abysmal. Half of the federal agency strategic plans make no mention of cybersecurity, and less than one quarter of IT objectives make any mention of efforts to secure IT systems. Additionally, federal agencies rarely discuss cybersecurity efforts in detail. Most agencies only have brief mentions of ongoing efforts.

The Department of Defense (DoD) is the notable exception. The DoD's strategic plan discusses a variety of efforts to continuously monitor and secure IT infrastructure. This includes building robust systems with multiple redundancies and authentication protocols. In addition, the plan discusses efforts to improve the security of its interoperable systems through the Joint Information Environment (JIE) initiative.

The vast majority of public agencies lack a clear cybersecurity plan. In addition, equally striking is the reactive nature of most plans when it comes to cybersecurity. In order to address the cybersecurity threat agencies need to be proactive and sense the evolving technology space. Agencies need to develop capabilities to take proactive stances when it comes to understanding future threats. This will require them to develop innovative cybersecurity strategies.

Protecting IT infrastructure may seem like a no-brainer, but it is clear that cybersecurity is not a high priority for most U.S. federal agencies. Failure to enhance IT security will likely result in catastrophic outcomes as militant groups and other cyber vandals increasingly target critical infrastructure.

Kevin C. Desouza
Nonresident Senior Fellow, Governance Studies, Center for Technology Innovation
@KevDesouza
Kevin C. Desouza is a nonresident senior fellow with the Center for Technology Innovation. He also serves as the associate dean for research at the College of Public Programs and is a professor in the School of Public Affairs at Arizona State University.
More Posts from Kevin > | View Expert Page >

Kena Fedorschak
He engages on policy driven research efforts at Arizona State University's Decision Theater Network. He is also pursuing his MBA at the W.P. Carey School of Business. Kena can be reached at kfedorschak@gmail.com
@kenafedorschak

Previous
« How to Improve the Intellectual Property System
Next
How to Make Health Information Exchange Platforms Sustainable »

TECHTANK

TechTank focuses on new developments in science and technology policy and how they affect health care, education, economic development, innovation, and governance. Our goals are to highlight new data and ideas, and provide commentary on science and technology trends in the United States and around the world.

View all blogs ›

CONTRIBUTORS TO THIS BLOG


Darrell M. West
Vice President and Director, Governance Studies
Founding Director, Center for Technology Innovation
@DarrWest


Stuart N. Brotman
Nonresident Senior Fellow, Governance Studies, Center for Technology Innovation

Cameron F. Kerry
Ann R. and Andrew H. Tisch Distinguished Visiting Fellow, Governance Studies, Center for Technology Innovation
@Cam_Kerry

Walter D. Valdivia
Fellow, Governance Studies, Center for Technology Innovation
@WalterdValdivia


Niam Yaraghi
Fellow, Governance Studies, Center for Technology Innovation
@niamyaraghi

Join the Conversation

Share your tech policy ideas
Email Us
#TechTank

Blog Roll

- AAAS SCIENCE INSIDER
- DIGITIMES
- FCC BLOG
- HILLICON VALLEY
- NEXTGOV
- NYT BITS BLOG
- OFFICE OF SCIENCE AND TECHNOLOGY POLICY
- OPEN TECHNOLOGY INSTITUTE
- RE/CODE
- TAP BLOG
- TECHCRUNCH
- TECHDIRT
- TECHNOLOGY POLICY INSTITUTE
- THE SWITCH
- THE VERGE
- WIRED

Most Viewed Blog Posts

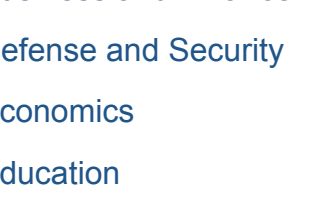
- WHY ARE INTEREST RATES SO LOW?
- WHY ARE INTEREST RATES SO LOW, PART 2: SECULAR STAGNATION
- INAUGURATING A NEW BLOG
- WHY ARE INTEREST RATES SO LOW, PART 3: THE GLOBAL SAVINGS GLUT
- GERMANY'S TRADE SURPLUS IS A PROBLEM

GET UPDATES
TechTank
Email Alerts
RSS Alerts

RELATED RESEARCH

BLOG POST
How state governments are addressing cybersecurity
March 5, 2015, Gregory Dawson and Kevin C. Desouza

MORE FROM GOVERNANCE STUDIES



BLOG POST
Alternative governance models for the air traffic control system: A user cooperative versus a government corporation
April 6, 2015, Dorothy Robyn

Governance Studies ›