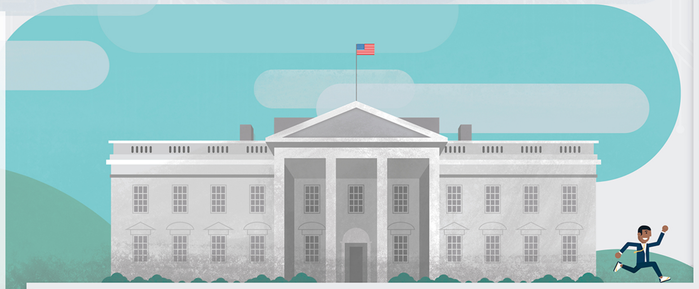
CYBERLAND

2015 was a long year of ups and downs for the federal government. With myriad hacks at OPM, the IRS, and DoD, it seemed that government was being attacked from all sides. But for every attack, federal agencies were swift to deploy countermeasures and the administration also began crafting proactive security plans to safeguard our IT infrastructure. It's been a long road of setbacks and progress. To understand this journey, take a walk with us through the Cyber Land of 2015.



START

= Cyber Attack

January

JAN. 12

U.S. Central Command's (CENTCOM) YouTube and Twitter accounts are hacked and defaced by the CyberCaliphate

February

6,000

U.S. Cyber Command reaches the halfway point toward its goal of reaching 6,000 personnel

FEB. 2

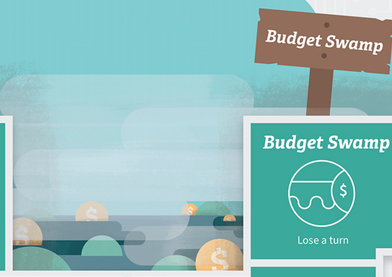
$14 billion

President Obama recommends $14 billion for cybersecurity efforts in the budget for Fiscal Year 2016, which is an 11 percent increase from the previous budget

Also in the FY 2016 budget, the administration proposes establishing a single federal standard for notifying individuals when private sector breaches occur, simplifying and standardizing the existing patchwork of 47 state laws that contain data breach report requirements into 1 federal statute

FEB. 10

White House announces the creation of a new agency, the Cyber Threat Intelligence Integration Center, to coordinate the cyber data collection, knowledge sharing, and coordination between other government agencies



Budget Swamp

Lose a turn

March

MAR. 13

The State Department disables large parts of its network to remove malware from Russian hackers in its unclassified email system. This was the second attempt at repairs from the ongoing cyber-attack. The first was in Nov. 2014

April

The Office of Personnel Management discovers a breach that occurred in late 2014

4.2 million

Ultimately it is revealed that 4.2 million people's information was compromised.

Hack Ridge

Return to start

APR. 24

Unknown hackers manipulate the domain name system of the Federal Reserve Bank of St. Louis to send users to rogue websites

May

MAY 26

334,000

IRS announces that criminals gained unauthorized access to information on more than 334,000 tax accounts through IRS' "Get Transcript" application

June

JUN. 8

Army.mil is taken offline for several hours after hackers, possibly from the Syrian electronic Army, gained access to the website and posted personal messages. No critical information was accessed

JUN. 10

The AnonGhost group defaces two subdomains of the U.S. Air Force

JUN. 12

Officials close to the OPM investigation uncover a second breach of computer systems containing information related to the background checks of former, current, and prospective federal employees

21.5 million

They eventually conclude 21.5 million people's information was stolen in this breach, including 3.6 million records related to people from the hack discovered in April

govloop

July

JUL. 25

4,000

Upon discovering a cyber breach caused by spear-phishing, the Pentagon Joint Chiefs of Staff's e-mail system for 4,000 employees is taken offline for 2 weeks

JUL. 23

4,200

Anonymous claims responsibility for leaking the personal information of the Census Bureau's 4,200 employees after gaining access to the Federal Audit Clearinghouse

Plains of Priority

Follow the path ahead

JUL. 17

Results from the federal 30-Day Cybersecurity Sprint are released, noting that:

JUL. 10

850,000

The Army National Guard announces a breach in cybersecurity after discovering a contract employee inadvertently transferred files with PII of around 850,000 current and former National Guard members to a non-DoD accredited data center

JUL. 9

The Cyber Islamic State defaces a subdomain of the Department of Energy's Argonne National Laboratory in Illinois

Security Meadows

Roll again

Federal CIO Tony Scott launches a government-wide Cybersecurity Sprint, giving agencies 30 days to beef up their cyber defenses around 8 priority areas

1. Protecting data
2. Improving situation awareness
3. Increasing cybersecurity proficiency
4. Increase awareness
5. Standardizing and automating processes
6. Controlling, containing, and recovering from incidents
7. Strengthening systems lifecycle security
8. Reducing attack surfaces

August

AUG. 28

76%

76% of civilian users are reported to be using Personal Identity Verification cards to access federal government networks

72%

Federal Civilian agencies increased their use of strong authentication for privileged and unprivileged users to 72 percent – an increase of 30 percent since last reports

75%

Federal civilian agencies increased their use of strong authentication for privileged users to 75 percent – an increase of more than 40 percent since last reports

Plains of Priority

OCT. 21

Office of Management and Budget releases for public comment the first revision in 15 years to OMB Circular No. A-130, which is the federal government's strategy for buying, managing and securing IT systems

OCT. 27

The Cybersecurity Information Sharing Act of 2015, which would allow Internet traffic information to be shared between the U.S. government and the private sector, passes the Senate

September

SEP. 30

15

15 agencies report meeting their Secure Configuration Management CAP Q3 target

14

14 agencies meet the anti-phishing and malware defense ("Blended Defense") CAP Q3 target

October

OCT. 19

The personal information of CIA Director John Brennan, DHS Secretary Jeh Johnson, and other current and former intelligence officials, as well as private email messages and addresses, are exposed after hackers accessed Brennan's private AOL account

Plains of Priority

Follow the path back

OCT. 30

The federal Cybersecurity Strategy and Implementation Plan (CSIP) is released, with focus on achieving 5 objectives:

1. Prioritized Identification and Protection of high-value information and assets
2. Timely Detection of and Rapid Response to cyber incidents
3. Rapid Recovery from incidents when they occur and Accelerated Adoption of lessons learned from the Sprint assessment
4. Recruitment and Retention of the most highly-qualified cybersecurity Workforce talent the Federal Government can bring to bear
5. Efficient and Effective Acquisition and Deployment of Existing and Emerging Technology

November

NOV. 4

23/24

23 out of 24 federal agencies receive an 'F' grade in at least one category on their FITARA* implementation scorecard

0

0 federal agencies receive an overall 'A' grade on their FITARA implementation scorecard

NOV. 10

1,000

OPM authorizes DHS to hire up to 1,000 new cybersecurity professionals

NOV. 13

Deadline for all federal agencies to identify and report their High Value Assets, according to CSIP

December

DEC. 1

OPM establishes a Cybersecurity Resource Center to help individuals whose information was stolen in previous agency breaches

DEC. 11

OPM completes initial mailing of notification letters to individuals impacted by earlier breaches

DEC. 31

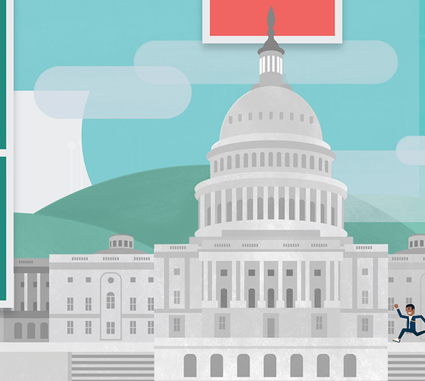
Deadline for NSC and OMB to release the EO 13681, Improving the Security of Consumer Financial Transactions implementation plan

NOV. 17

19

The Department of Interior publicly announces that foreign intelligence agents and other hackers attacked the agency's network 19 times over the past few years to obtain unknown amounts of stolen data

FINISH



Sources: whitehouse.gov | dhs.gov | oversight.house.gov | performance.gov | dlapiper.com | nationalguard.mil | crn.com | hackmageddon.com | gpo.gov