Rebuilding Trust In Government: The Role Of Security

Authenticating email is about more than security, it is about restoring trust in the government.

By **John Wilson**
Field Chief Technology Officer
Agari

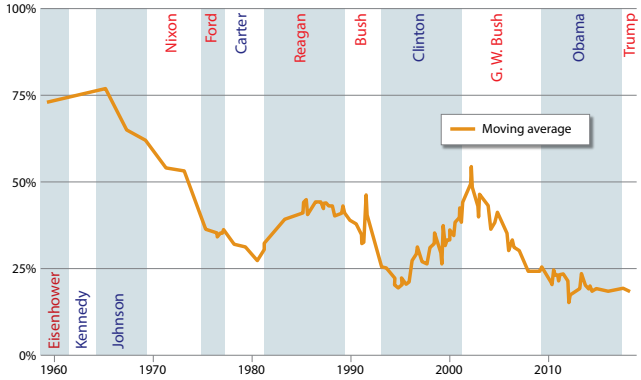
Historical research shows that U.S. citizens' trust in the government continues to languish at all-time lows. Amidst these challenging times, cybersecurity professionals at Federal agencies have a rare opportunity to step up and play an even more strategic role as the U.S. government strives to regain the trust of its people. The recent Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-01, which mandates the adoption of a critical email authentication standard called DMARC, is shining yet another spotlight on the important role that IT security teams play in keeping our government's communications, operations and identities secure.

The question is, how will the Federal cybersecurity community respond?

Trust in Government at Historic Lows

According to data from the Pew Research Center, public trust in the government remains near historic lows. Only 18% of Americans today say they can trust the government in Washington to do what is right "just about always" (3%) or "most of the time" (15%). Distrust in government is certainly nothing new. Since this data was first recorded back in 1958, trust in government has gradually eroded over time, with a few notable peaks during the economic boom of the 1980s and again during moments of national unity after 9/11. (See chart below.)

Public trust in government near historic lows
% who trust the government in Washington always or most of the time



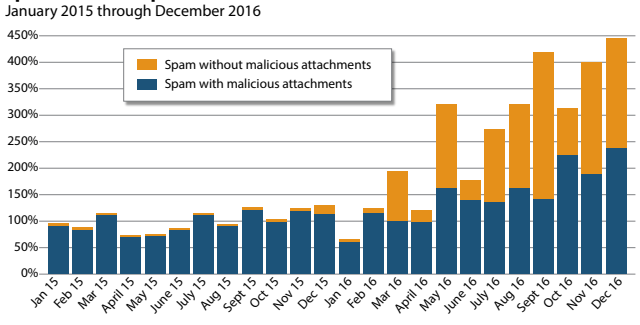
Whatever the politics and perceptions driving this trend, the fact remains that the U.S. government has struggled with a crisis of confidence. It is against this backdrop that the U.S. government is facing another struggle that impacts public trust — cybersecurity, and specifically, identity deception.

Federal Government at Risk for Mass-Scale Identity Deception

Whether it's spear-phishing, targeted email attacks, or some other form identity deception, email remains the number one weapon of choice for cybercriminals. KPMG determined in a 2017 study that 91% of all cyber-attacks involve spear-phishing. And in that same year, according to Verizon's 2017 Data Breach Investigations Report, 67% of all malware breached the organization via email attachments that people were tricked into clicking on.

Sadly, the trend is only growing worse. The IBM Threat Intelligence Index 2017 report shows the dramatic rise not only in spam over the years, but specifically spam with malicious attachments. (See chart below.)

Spam volume and spam with malicious attachments
January 2015 through December 2016



Federal agencies are particularly vulnerable to this form of attack, as the vast majority of communications both within an agency, with other agencies and with their citizenry take place via email. This is why the DHS has mandated the adoption of DMARC, a proven and effective defense against malicious spam and phishing. DHS BOD 18-01 creates more than a requirement for compliance. It also creates an opportunity for strategic leadership.

DHS BOD 18-01: A Moment in Time for the Federal Cybersecurity Community

The majority of people in the U.S. don't think the government is either capable or willing to do what it needs to do to function properly. Imagine if the average tax-paying citizen understood the current inability to distinguish legitimate and fraudulent emails purporting to originate from their government. What sort of impact is ***that*** going to have on the people's trust?

DMARC is about much more than simply securing emails. It's about securing the trust of the people who rely on the services their government provides. In that spirit, here are three specific recommendations for what Federal cybersecurity professionals can do immediately to help rebuild trust in our Federal government and the people who operate it.

1. Educate your internal teams. How many people in your organization know what DHS BOD 18-01 is or why it's important? How many know what spear-phishing is and what a pervasive threat it is? How many people understand the tireless work that happens behind the scenes to prevent those kinds of attacks? People should be made aware of what the threat is, the consequences of falling prey to that threat, and what their local cybersecurity teams are doing to keep them and the public safe.

2. Educate your citizenry. Have fail-safes in place to immediately communicate with your constituency in the event of an identity breach. Be ready to coach your internal and external audiences on what to do in the event of fraudulent communication. Let them know what solutions you are putting in place to protect against this eventuality. Waiting until after a devastating phishing attack is not the best time to start communicating with the citizens who pay your department's bills. Start that conversation before there's any further erosion of trust.

3. Trust your DHS BOD 18-01 compliance to a proven solution. The good news is there is a proven effective solution available. In fact, 9 out of 10 DMARC-protected Federal domains already use Agari. These trail-blazers have already laid the groundwork for where and how to implement the best protections against spear phishing, spam and email-borne cyberattacks. Other Federal cybersecurity professionals can benefit from their experiences. For best practices on Federal Government DMARC implementation, please visit www.agari.com/Federal. The Agari Email Trust Platform is the industry's only artificial intelligence (AI) driven defense system that automates the detection of digital deception, modeling authentic, trustworthy communications to protect humans from being deceived by cyberattacks such as phishing, ransomware and business email compromise (BEC). ■

SOLUTION FOCUS

Agari's Email Trust Platform

Today, companies are most vulnerable to cyber-attacks that prey on human perception and identity deception, with email as the current attack vector.

The Agari Email Trust Platform protects against the pervasive threat of digital deception.

Common forms of digital deception include display name fraud, domain name fraud and look-alike domain fraud. These forms of digital deception are leveraged in malicious inbound attacks, including spear phishing, business email compromise (BEC), and ransomware. Digital deception also takes the form of outbound phishing and spam, resulting in negative brand reputation.

The Agari Email Trust Platform protects both inbound and outbound email communication from digital deception to secure the enterprise, to improve productivity and to preserve brand reputation.

By automating the detection of digital deception, the Agari platform eliminates the vulnerability of human perception as the root cause of email security risk. Agari also streamlines the deployment and implementation of DMARC, an email authentication standard, with centralized management, automated sender discovery and analytics.

The Agari Email Trust Platform is the industry's only artificial intelligence (AI) driven defense system that automates the detection of digital deception, modeling authentic, trustworthy communications to protect humans from being deceived by cyberattacks such as phishing, ransomware and business email compromise (BEC).

To learn more, visit www.agari.com/federal.