FEDERAL CYBERSECURITY THREAT SURVEY REPORT
What to do when you can’t modernize fast enough
The 2017 CIA Wikileaks, 2015 and 2016 IRS and 2015 OPM breaches have one thing in common: The criminals compromised federal systems, exposing highly confidential and valuable information. And, according to the Privacy Rights Clearinghouse\(^1\), these three breaches are just the tip of the iceberg.

What’s going on? Why are these breaches happening, and what is enabling them? To find out, BeyondTrust commissioned a survey of senior Federal IT managers in early 2017.

The survey exposes an environment where outdated infrastructure is a significant cause for concern among Federal IT professionals and can lead to serious breaches.

**What Worries Federal IT Managers?**

When asked to name the top risks they face, federal IT professionals cited application vulnerabilities, nation-state attacks and malware. This should come as no surprise as many data breaches are the result of an attacker gaining access to a system (through a compromised password or known vulnerability), and moving laterally throughout an environment until their objective is achieved, oftentimes planting malware that enables communication to a command control server.

\(^1\) Privacy Rights Clearinghouse Data Breaches, Government [https://www.privacyrights.org/data-breaches?title=&org_type%5B%5D=257](https://www.privacyrights.org/data-breaches?title=&org_type%5B%5D=257)
What are Federal IT Managers Doing Today to Combat Cyber Risks?

We then asked respondents what tools were most important to them in terms of securing their information environment. Here they ranked privileged access management and vulnerability patching as most important. This is significant as these technologies restrict user privileges and close off security weaknesses in systems.

Yet, despite understanding the importance of such measures, most (56 percent) use alternate solutions to manage privileged passwords and nearly two-thirds (63 percent) report less than fully mature vulnerability remediation programs. In fact, 6 percent have NO remediation plan, and another 14 percent do only the bare minimum required by compliance mandates.
Aging Infrastructure Leads to Costly Breaches

Aging infrastructure can make federal systems more vulnerable to attack. How common are breaches in the federal government? Forty-two percent of those surveyed have experienced a data breach within the past six months. A staggering one in eight has experienced a data breach within the past 30 days.

Put another way; the typical federal IT system experiences one breach every 347 days.

These breaches are costly. Respondents report that the typical data breach costs more than $91,000. Of course, this is just the average. The highest profile breaches can run into the millions of dollars in damages.

When you consider that OPM estimates there are roughly 7,000 federal systems in use, the annual cost due to data breaches is $637 million every year. The most frequently reported costs include loss of productivity, loss of reputation and pure monetary damages.

Why haven’t federal IT organizations made more progress in combatting cyber threats?
An Aging Federal IT Infrastructure Breeds Risk

An overwhelming majority of Federal IT managers (81 percent) say aging IT infrastructures have a somewhat to extremely large impact on their cybersecurity risk. Further, three of five (61 percent) say aging infrastructure is a roadblock to achieving federal cyber security mandate compliance.

We found ample examples of aging infrastructure in our survey. For example, a surprising 47 percent of Federal agencies still use Windows XP, driving a third of respondents (35 percent) to report that this kind of aging infrastructure had a somewhat to large impact on their ability to affect vulnerability patching.
Looking Towards the Future
Going forward, federal IT decision makers plan to employ automation, cloud, and “as-a-service” technologies to achieve IT modernization. These are budget-friendly initiatives, which is important as most (81 percent) say budget is a constraint.

The top three items they’ll be automating include threat analytics, vulnerability risk scoring and application patch management.
How Can Federal Agencies Address These Threats?

The BeyondTrust 2017 U.S. federal government study points to four best practices that any agency can implement.

1. Manage privileged credentials with greater discipline, eliminate administrator rights and enforce least privilege

Thirty percent of respondents believe that insider threats pose a significant threat and 35 percent believe their users have more privileges than are required. To mitigate insider threats and the exploitation of privileges, adopt a least privilege model by removing admin rights from users and storing all privileged credentials in a secure safe. *Known escalation attacks have been around for years* and are still being used. These attacks require local administrator rights. It’s not just about insiders. Enforcing least privilege prevents lateral movement within an organization if a breach does occur.
Isolate legacy systems to reduce attack surfaces

Modernization of federal IT infrastructure is a priority for most survey respondents, but realistically this will not happen quickly. These aging systems have known risks. Reduce the attack surface by isolating legacy systems. Segment these systems to force all traffic through a proxy to reduce attack vectors. Deploy an automated password and session management solution that provides secure access control, auditing, alerting and recording for any privileged account. This will provide segmented access to critical systems, manage passwords, and monitor when tasks and operations are committed to a managed system.
Improve the maturity of vulnerability management through automated patching

Even in today’s sophisticated threat landscape, the majority of attacks target known vulnerabilities that can be easily patched. Effective patch management goes a long way in reducing a network’s overall attack surface. To be truly effective, patch management requires intelligent prioritization and broad coverage for common business applications. To improve the efficiency and effectiveness of an agency patch process deploy a solution that provides integrated, automated patching. Implementing a solution that delivers analytics and trending across the threat lifecycle for multi-dimensional reports on assets, vulnerabilities, attacks and remediation allows prioritized patch management based on risk profile.
Unite threat intelligence from multiple sources to better prioritize risks across the environment

Since the asset risk-to-user privilege risk pattern is a common attack vector, deploy solutions that correlate asset-based risk with user-based activity to gain a more complete picture of risks, gaining needed prioritization of the most impactful risks. For example, advanced persistent threats (APTs) can be analyzed against privileged password, user, and account activity, along with asset characteristics such as vulnerability count, vulnerability level, attacks detected, risk score, applications, services, software and ports. Consuming multiple data feeds from in-place solutions into a single console can help mitigate additional costs and reduce complexity.
Act Now to Protect Aging Infrastructure

The Federal Information Technology landscape is complicated. Today, aging custom built systems still house mission critical information. In fact, 69 percent of our survey respondents indicated the risk of taking these systems down could outweigh the risk and cost of maintaining them. Budget for modernization is limited, getting things done takes time and leadership changes often result in shifting strategies and priorities. Unfortunately, this aging infrastructure continues to expose agencies to an increased risk of data breaches.

Recognizing this problem has led federal IT managers to rate IT modernization as their top initiative. In fact, White House homeland security adviser Thomas Bossert recently addressed the issue, saying

“Federal networks at this point can no longer sustain themselves. We cannot tolerate indefensible technology, outdated, antiquated hardware and software. Modernization is absolutely critical.”

Across all levels of government, the search is on for an innovative way to modernize these systems. Yet, while modernization proceeds the risks will remain. By following the best practices listed in this guide, federal agencies can mitigate risk in their legacy systems while migrating to a more modern information technology environment.

2 https://www.fedscoop.com/white-house-adviser-promises-funding-centralization-federal-cybersecurity/
Federal IT: The Road to Modernization

Methodology
According to the Privacy Rights Clearinghouse, the 2017-2018 Wikileaks, 2015 and 2016 Wikileaks, and 2015-2016 DRPM breaches, one thing in common is that breaches are just the tip of the iceberg.

Why are these breaches happening and what is enabling them?
To find out, BeyondTrust commissioned a survey of 195 senior Federal IT managers involved with privileged access management in early 2017.

What Worries Federal IT Managers?

Top Concerns
- Application Vulnerabilities
- Nation-State Attacks
- Malware

What are Federal IT Managers Doing Today to Combat Cyber Risks?

Aging Infrastructure Leads to Costly Breaches
- Nearly three-fourths of federal agencies place access management as a somewhat to extremely important initiative (second highest priority)
- Nearly 42% of agencies have reported at least one breach within the last 2 years

An Aging Federal IT Infrastructure Breeds Risk
- One in four have experienced 3 or more breaches within the past 2 years
- 39% of respondents say their ability to achieve their mission is somewhat or greatly impeded by aging IT infrastructure

There is danger lurking within the Federal Government's outdated infrastructure.
Download our full 2017 BeyondTrust Federal Cyber-Security Threat Survey Report to learn the four best practices any agency can implement to mitigate these risks today.

Source: BeyondTrust
https://www.beyondtrust.com/aging-fed-it-risky