WHAT IF...WE COULD TIP THE BALANCE OF POWER?
Consider this: Warren Buffett, one of the most successful investors of our time, recently said that cyberattacks are the “number one problem with mankind.” That is a bold statement and captures what is felt across the entire Federal landscape every day. According to 2016 findings by the Government Accountability Office (GAO), cyberattacks on our federal government have shot up by 1,300 percent since 2006\(^1\). Not surprisingly, given recent events, a Pew Research Center study reported that roughly half of Americans don’t trust the Federal government to protect their data\(^2\).

Although the balance of power may always be in favor of our cyber adversaries, it is time to tip the scales in our direction. Our defense needs to be strong every time, all the time.
Cyber threats against our government are a danger to the U.S. on the same level as terrorism—and in some cases are one and the same. Cyber intruders relentlessly scheme to breach, steal, and destroy—actions that have very tangible and devastating effects. All of this is made worse by the fact that cyber is a frictionless, or easily adapted, weapon system—once a hack is published or a breach is discovered, it’s game on for the adversaries within moments.

The WannaCry ransomware computer virus is the latest example of both the frictionless nature of cyber weapons and how adversaries attack vulnerabilities and create chaos around the world. WannaCry had a far-reaching impact, with estimates demonstrating that over 200,000 computers were infected across at least 150 countries. Over 70,000 medical devices were affected, including MRI scanners and blood-storage refrigerators, posing a severe threat to human lives. Now, enhanced versions of WannaCry are emerging, enriched by hackers who study and build on previous releases to harden the code and increase the ransomware’s destructive power.

The increasingly interconnected nature of the Internet and the explosive growth of IoT have created new opportunities for threats and malicious behavior. Witness the 2016 Mirai botnet, which aggressively targeted Internet infrastructure giant—Dyn. This attack is likely just the first of many to come. During the Cold War, we were concerned about MAD—Mutually Assured Destruction. Today, we are facing a new MAD—Mutually Assured Darkness.

Federal agencies must take swift, decisive actions to protect their information systems. Otherwise, these agencies risk losing sensitive information, exposing vulnerabilities in our security and leaving taxpayers saddled with hundreds of millions of dollars in damages.

The Administration has an opportunity to gain the advantage by resetting the federal government’s cybersecurity posture. From the outset, this Administration has been confronting a full range of global cyber threats that were nearly unthinkable eight years ago. The threat is urgent and in response, the White House is mandating that Federal Agency leaders be held accountable for cybersecurity in a way that was once the province of technical officials.

Protecting the Federal government must start at the very top, and the recent Presidential Executive Order Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure gives agency leaders strong impetus to act now.

Federal agencies are actively conducting audits to establish inventories of their data focusing on defining their High Value Assets (HVAs) or “crown jewels.” In addition, agencies are actively scanning and fixing vulnerabilities within information systems to ensure that those HVAs and other data are less exposed and more secure.
BEYOND THESE ACTIVITIES, AND TO TRULY TIP THE BALANCE OF POWER IN OUR FAVOR, WE RECOMMEND:

**HUNT**

**Review, Engage, Repeat—Outsmart Adversaries**
Agencies must engage in a constant, persistent hunt for malicious activity and embrace a purposeful and ongoing approach to cybersecurity. A proactive, intelligent defense approach is the best way to maintain the highest levels of security confidence and reduce detection times from months to hours.

**DEFEND**

**New Focus on Data Security—Security from the Inside-Out**
Agencies must take a multi-layered approach to protecting their data which will eliminate the "soft, chewy center." This approach entails adding on layers of protection through encryption and obfuscation mechanisms controlled by strong, yet flexible identity and access management.

**Leverage Shared Services and Cloud Capabilities to Reduce Scope**
Agencies are able to reduce their overall scope by leveraging shared services and cloud capabilities. Reputable cloud providers see security as existential responsibility and can take on the basic blocking and tackling.

**OUTSMART**

**Develop New Playbooks to Find and Expel Attackers**
Practice cyber response using advanced cyber threat emulation playbooks and a sophisticated sparring partner to evaluate your readiness posture, skills of your people, and susceptibility to potential “Darkness” when you are attacked. Formulate off-line ways to do business, when needed.

**Design for Cyber Resiliency**
Given that absolute security is absolutely impossible, and a cyber event will occur, next generation IT systems must be designed to be cyber resilient. By leveraging advanced cloud features and software-defined networking, compute, and storage, Agencies can deliver future IT environments that are able to dynamically isolate affected systems and immediately reconstitute from clean resources to ensure that mission and business operations are unaffected.
START CLEAN, **STAY CLEAN**

The new Executive Order sets the stage for a change in our cybersecurity posture. It is a critical moment to rebuild our cybersecurity. Now is the time to develop a more aggressive approach.

Installing the basics, such as the equivalent of home alarms, and waiting for the adversaries to trip them is not enough. It can take months to detect a cyber intrusion, but continuous scanning, especially around high-priority assets, will enable faster detection and removal of problems.

A focus on **starting with a clean environment** to restore confidence in our government networks is critical. This enables security professionals to focus on long-term security planning and scalable solutions.

The face, strategy and intent of our adversaries are always changing, making it essential to move beyond a “traditional” approach to security. Cybersecurity has to evolve with the threat, and must be viewed as a core responsibility for all leaders across government.

SHIFTING THE BALANCE OF POWER—**REBUILDING CYBERSECURITY**

Shifting the balance of power away from adversaries requires a change in approach. In order to establish a strong posture: **Hunt, Defend, Outsmart**. Get ahead of the issue. Always assume that our networks are at risk, and run toward the problem. For our safety and the safety of our networks, engage in a proactive intelligent defense.
ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 401,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE FEDERAL SERVICES

Accenture Federal Services is a wholly owned subsidiary of Accenture LLP, a U.S. company, with offices in Arlington, Virginia. Accenture’s federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations.