GLASSWALL

U.S. Federal Government IT Modernization:
Run Smarter, Not Faster

"Well, in our country," said Alice, still panting a little, "you'd generally get to somewhere else—if you ran very fast for a long time, as we've been doing."

"A slow sort of country!" said the Queen. "Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!"

- Lewis Carroll, *Through the Looking-Glass*

Introduction

Information security often feels a lot like the Wonderland experienced by Alice. Reality can be elusive and what was once real can quickly become fiction. Information technology, or IT, and its use-cases are constantly evolving. Unanticipated vulnerabilities emerge within software, networks and supply chains. Threat actors exploit new and old methods to access their targets. And the volume and velocity of these events ebb and flow, although appear to only trend in one direction. At the same time, the practice of information security is not stagnant. The technologies, processes and tradecraft of information security professionals continues to evolve alongside that which they protect and those against whom they offer their protection. The challenge is undertaking security as intelligently as possible, using data-driven, risk-informed strategic occasions to apply resources as efficiently and effectively as possible. Malicious actors often achieve large consequences through the application of a comparatively small perturbation to a victim's environment—their effects scale far beyond their efforts. With less exertion, these actors run far faster than those defending against them. Security professionals need to take advantage of similar opportunities to achieve success at scale. The IT modernization effort taking root within the U.S. federal government presents just such an opportunity.

Impetus for IT Modernization

For too long, our adversaries in cyberspace have been running circles around U.S. and allied government defenses. This is partially due to the advantages afforded the offense, such as those identified by the SANS Institute in 2002 that still ring true: networking, focused attacks, weaknesses of defense, jurisdictional and prosecutorial advantages, and the inherent desire of humans to trust[1]. However, neither the government nor private sector have treated the problem as comprehensively as possible. In Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," a critically important finding is that "[t]he executive branch has for too long accepted antiquated and difficult–to-defend IT."[2] This finding, coupled with a subsequent observation that risk management needs to involve planning focused on maintaining, improving and modernizing IT, is important in that it forms the basis for the implementation of an IT modernization policy across the U.S. government. Of course, the need to modernize the U.S. government's legacy IT infrastructure is not a new realization. Since at least 2012, the U.S. Government Accountability Office (GAO) has reported on challenges associated with the oversight of legacy IT.[3] Recently, GAO's David Powner testified that federal agencies experience greater vulnerability due to a history of overlooking security so long as a system operated as designed and supported the agency mission or mission support function for which it was acquired.[4] Of course, Mr. Powner's testimony was not surprising given the U.S. government's efforts with IT modernization over the prior three years.

Previously, the U.S. Office of Management and Budget (OMB) observed that legacy systems make agencies vulnerable. Specifically, in the aftermath cyber intrusions at the U.S. Office of Personnel Management, OMB noted "…several fundamental challenges exist which hinder progress in eliminating cybersecurity risks. Among these challenges is a broad surface area of legacy systems with thousands of different hardware and software configurations across the Federal Government, which introduces significant vulnerabilities and opportunities for exploitation."[5] The U.S. House of Representatives Oversight and Government Reform Committee's report on the OPM breach offered even greater specificity as to the potential negative impact legacy IT systems can have on an agency, its mission functions and the citizens who depend on those functions.

In its report, the House committee warned that "[t] he state of OPM's IT legacy environment leading up to the 2014 and 2015 breaches illustrates the pressing need for federal agencies to modernize legacy IT in order to mitigate the cybersecurity threat inherent in unsupported, end of life IT systems and applications."[6] Testimony from multiple government officials and documents produced in response to the committee's investigation noted the existence of out of service hardware, software that could no longer be patched, the absence of encryption and a lack of multifactor authentication on the targeted systems such that encryption would not have mattered—the intruders were using valid user credentials.

---

1 SANS Institute, An Uneven Playing Field: The Advantages of the Cyber Criminal vs. Law Enforcement-and Some Practical, 2002. Accessed June 25, 2018 at < https://www.sans.org/reading-room/whitepapers/legal/uneven-playing-field-advantages-cyber-criminal-vs-law-enforcement-and-practica-115>.

2 President Donald J. Trump, Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017. Accessed June 13, 2018 at <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.

3 See, e.g., GAO, "Information Technology: Agencies Need to Strengthen Oversight of Billions of Dollars in Operations and Maintenance Investments," GAO-13-87 (Washington, D.C.: Oct. 16, 2012); GAO, "Information Technology: Agencies Need to Strengthen Oversight of Multibillion Dollar Investments in Operations and Maintenance," GAO-14-66 (Washington, D.C.: Nov. 6, 2013); and GAO, testimony of David A. Powner, "Information Technology: Federal Agencies Need to Address Aging Legacy Systems," GAO-16-696T (Washington, D.C.: May 25, 2016).

4 Hearing on "State of Play: Federal IT in 2018" before the Subcommittees on Information Technology and Government Operations, Oversight and Government Reform Committee of the U.S. House of Representatives (March 14, 2018).

5 U.S. Office of Management and Budget, Memorandum M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" (Washington, D.C.: Oct. 30, 2015). Accessed June 14, 2018 at < https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf>.

6 Committee on Oversight and Government Reform, U.S. House of Representatives, Majority Report, "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation" (Sep. 7, 2016), p. 195.

If prior incidents suggested an impetus for incremental improvements in federal agency information security, the OPM breaches rocked the U.S. government into a realization that holistic change was necessary. While OMB and the National Security Council staff in the Executive Office of the President, the Department of Homeland Security, the Department of Defense, the National Institute of Standards and Technology and the U.S. General Services Administration led a series of responsive information security initiatives during the last year of the Obama Administration, the Trump Administration picked up the torch with EO 13800 in May 2017. Unlike other areas of U.S. national policy, where administration changes (especially involving a change in political parties) lead to discontinuity, U.S. cybersecurity policy tends to experience general continuity. Just as President Obama continued and enhanced the Comprehensive National Cybersecurity Initiative and other policies initiated by President Bush, President Trump is building on fundamental IT and cybersecurity policy changes started by President Obama.

Ready…Recent USG Efforts

The U.S. government needs to ready itself to run the race of its choosing, not the course dictated by malicious actors. As previously discussed, EO 13800 set the foundation and direction for the Trump Administration's approach to U.S. federal government IT modernization. Among its primary action items was direction for a report on federal government IT modernization to be coordinated by the American Technology Council and authored by the Secretary of Homeland Security, the Director of OMB and the Administrator of the General Services Administration. Importantly, the IT modernization report was not to be completed and delivered in a vacuum. In parallel to the American Technology Council-led effort, each Federal agency was tasked to complete a risk management report. Delivered to OMB and DHS, those reports formed the foundation for a government-wide approach to improved cyber risk management.

Report to the President on Federal IT Modernization

The 2017 IT modernization report identifies a few current challenges to federal government IT efficiency and security. These challenges include a focus on perimeter-based security, an overreliance on physical, network-based protections, multiple independent agency actions to acquire and maintain IT solutions, and the federated use of cybersecurity products and services. The overall impact is a U.S. federal government "enterprise" that is unable to take full advantage of the IT and security scaling opportunities afforded by cloud environments, whole-of-government purchasing power and coordinated security certification and accreditation efforts that, taken together, would eliminate contracting, investment and process redundancies. Furthermore, eliminating these challenges would release resources that could be better focused on operating, maintaining and securing government IT.

The report includes a set of future state objectives and an implementation plan to attain them. At a high level, the implementation plan is designed to focus security protections closer to applications and data while similarly hunting for threats and vulnerabilities at that level of abstraction. In parallel, the report envisions increased use of shared services for non-mission specific functions, commodity IT, such as email, productivity tools and security solutions. This would occur in and across commercial cloud environments while avoiding "vendor lock-in". It would be supported by removing policy, budgeting, and acquisition guideline impediments to the adoption of shared services in cloud environments.

Both parallel efforts envision a degree of sequencing. Modernization would begin with the government's high-value assets. Revisions to current DHS-led perimeter protection policies and implementations would eliminate some barriers to cloud service migration. And overall acquisition and management of federal agency networks would be consolidated using GSA's Enterprise Infrastructure Solutions contract vehicle while providing flexibility to agencies as they avail themselves of the solutions offered by that vehicle. At the same time, the focus on cloud service adoption will begin with matching agency needs to the various models of cloud offerings. The adoption of email and collaboration tools in cloud environments would be accelerated. Finally, the government will improve upon and add to current shared security services, including through the Continuous Diagnostics and Mitigation (CDM) program and the security operations center (SOC)-as-a-service concept.

The improvements envisioned by the IT modernization report to the President will directly address two key findings and support resolution of a third finding contained in the "Federal Cybersecurity Risk Determination Report and Action Plan" required by Executive Order 13800.

Federal Cybersecurity Risk Determination Report and Action Plan

The Office of Management and Budget and DHS report that out of 96 agencies, only 25 are manging their cybersecurity risk. Yet, they also note that federal agency spending across the NIST Cybersecurity Framework functions is expected to have increased by $700 million from FY2016 to FY2017. According to the report, this spending occurred absent "a sense of prioritization or actual return on investment in terms of reducing cyber risks."[7] This is an obvious cause and symptom of running as fast as the appropriations and acquisitions cycles permit, but without running smart. Fortunately, Executive Order 13800 and the first action out of the risk report offer a solution. As agencies combine the use of the NIST Cybersecurity Framework, the U.S. government Cyber Threat Framework and NIST SP 800-39, "Managing Information Security Risk", they should be much better positioned to prioritize investments, assuming the availability of threat, vulnerability, consequence, and cost data to populate the espoused frameworks. This is a large assumption as the OMB report also recognizes that federal agencies do not have remotely standardized cybersecurity processes or IT capabilities. Nevertheless, IT modernization is likely to support this initiative as data collection can be built into new IT tools while the investment process itself will reinforce the need for agencies to adopt the full cyber risk management lifecycle articulated in the risk report.

Directly aligned with the IT modernization report's implementing actions, the second action item from the risk report envisions agencies continuing to standardize IT investments and cybersecurity capabilities. Three initiatives are specifically identified. First, agencies will continue to focus on improving identity, credentialing and access management, a critical deficiency that contributed to the OPM data breaches. Second, agencies will continue to consolidate and standardize their email services. The focus placed on this activity within the IT modernization report should ensure ongoing agency leadership attention around this effort. Finally, the action item encourages standardized software and applications through the larger focus on shared services, governmentwide marketplaces and the common configurations they can support.

The third action is designed to improve agencies' network visibility, including their ability to detect exfiltration of data. The two major thrusts of this action item focus on consolidating multiple SOCs within an agency to achieve a centralized SOC while also pursuing the SOC-as-a-service concept introduced in the IT modernization report. Visibility and SOC services can benefit greatly from increased use of cloud services if they are implemented with such benefits in mind.

Governance is one of the greatest challenges to effective cybersecurity. This is especially true within the U.S. government as DHS has previously reported in its annual strategic reviews required by the Government Performance and Results Act Modernization Act (GPRAMA).[8] The fourth action identified in the risk report is designed to improve governance within each agency. It reiterates the requirement set forth in the Federal Information Security Modernization Act of 2014 (FISMA) and Executive Order 13800 that agency heads are responsible for the cybersecurity of their agencies and the associated governance and risk management approaches undertaken in support of their agencies' missions. Successful implementation of the IT modernization report's initiatives is heavily dependent on governance and agency leaders. As such, the action items in the IT modernization report and the risk report should be mutually reinforcing.

Of course, one challenge with government policy can be a lack of resources to support implementation. While this often takes the form of insufficient budget, it also can result from insufficient or outdated legal authorities, particularly, those regarding U.S. federal acquisitions.[9] With respect to IT modernization and cyber risk management, most indicators suggest the U.S. federal government is well-positioned to move from planning into implementation.

---

7 OMB, "Federal Cybersecurity Risk Determination Report and Action Plan" (May 2018), p. 8.

8 See, e.g., the strategic review for DHS Goal 4.2 in DHS, "Annual Performance Report, Fiscal Years 2016-2018", p. 60. Accessed June 18, 2018 at: <https://www.dhs.gov/sites/default/files/publications/DHS%20FY%202016-2018%20APR.pdf>.

9 Kate Charlet, Harvard Kennedy School Belfer Center for Science and International Affairs, Understanding Federal Cybersecurity, April 2018, pp. 40-41. Accessed June 25, 2018 at <https://www.belfercenter.org/sites /default/files/files/publication/Understanding%20Federal%20Cybersecurity%2004-2018_0.pdf>.

Set...Hey, This Thing has Legs

Running smart requires a coordinated application of government resources based on risk-informed decisions and considerations of efficiency and measurable effectiveness. Similar to the policy and statutory machinations that enabled DHS's implementation of automated indicator sharing, IT modernization and cyber risk management will benefit from legislation that became law in the midst of implementing pre-existing Executive branch policy consistent with the statute. The Modernizing Government Technology (MGT) Act, enacted December 12, 2017 as part of the Fiscal Year 2018 National Defense Authorization Act, empowers individual federal agencies and the overall federal enterprise to strategically consider modernization investments and to resource them. For individual Chief Financial Officer Act agencies, it authorizes them to establish IT working capital funds (WCF). Also, it establishes a centralized Technology Modernization Fund and a related Technology Modernization Board. Whereas the fund is authorized up to $250 million in each of Fiscal Year 2018 and 2019, subject to appropriations,[10] the board's role is to evaluate proposals and make recommendations on projects requesting use of the fund.

The Office of Management and Budget released OMB M-18-12, "Implementation of the Modernizing Government Technology Act", in February 2018, which provides guidance to agencies regarding their individual IT working capital funds, establishes the board members and highlights the process for submitting project proposals. To assist agencies, the memorandum includes a template for project proposals. The board consists of seven members, including the Administrator of OMB's E-Government Office, a senior GSA official, a member from DHS's National Protection and Programs Directorate, and four members from federal agencies who are appointed by the OMB Director and are expected to have expertise in IT development, financial management, cybersecurity and privacy, and acquisitions. The inclusion of the DHS representative is essential to ensuring the linkage between MGT Act implementation, IT modernization efforts under Executive Order 13800, and the risk-based cybersecurity initiatives outlined in the risk report. The selected individual leads the team that worked closely with OMB on the risk report, was heavily involved in the IT modernization report and oversees the operational aspects of federal enterprise performance under FISMA while providing agencies with security assessments and

architecture design support. On June 7, 2018, OMB announced the first awards from the centralized fund, which totalled $45 million and went to the Department of Housing and Urban Development, the Department of Energy and the Department of Agriculture.

Sustained attention at the highest levels of White House and federal agency leadership also are needed to achieve meaningful impacts from IT modernization and cyber risk management. The change needed and sought by the federal government includes some quick-wins, but also involves multi-year investments in technology, people and processes. Fortunately, one of the key focus areas in the President's Management Agenda is IT modernization and cybersecurity improvements. It aligns Executive Order 13800 policy, MGT Act implementation and a GPRAMA Cross-Agency Priority Goal, "Modernize IT to Increase Productivity and Security", with associated metrics. Although this is an excellent foundation, a further enhancement would be for the Administration to work with the GAO's Director for Information Security Issues to align these initiatives with the indicators of improved risk management highlighted around federal agency cybersecurity in GAO's latest high-risk report.[11] Additionally, DHS should lead other agencies in considering how the IT modernization efforts currently underway, and the associated processes and governance structures, can accommodate and support the President's National Security Telecommunications Advisory Committee (NSTAC) focus on a cybersecurity "moonshot" that will dramatically change cybersecurity over the next ten years. Working with the NSTAC Cybersecurity Moonshot Subcommittee, the government can ensure that modernization and risk management improvements benefit from a whole-of-nation effort.

---

[10] In FY 2018, $100 million was appropriated for this fund.

[11] Accessed June 19, 2018 at: <https://www.gao.gov/highrisk/ensuring_the_security_federal_government_information_systems/why_did_study>.

Readying for the Run, Stretch Your Legs and Mind

Running smart requires more than the sheer muscle provided by variations on a common technology theme—it requires innovative technologies, people, processes, and practices. As the U.S. government implements IT modernization, it is important that the aperture is wide enough to look beyond only new technology. It also should include modernizing risk management and governance, standards and practices, and the workforce expected to use and secure a modernized IT infrastructure. As the risk report to the President notes, the government needs to "implement a timely approach for communicating cyber threats and risks, and for appropriately prioritizing the people, processes, and technology resources necessary to defend agency networks."[12] The interdependencies among these resources cannot be overstated. Therefore, modernization efforts need to solve current problems while remaining sufficiently anticipatory—for example, anticipating future human capital requirements, standards, and practices, which may change quickly based on the introduction of new technologies.

Instead of identifying the security tools of today in the context of current standards and best practices, IT modernization and the MGT Act board should stretch its mind—and encourage agencies to follow suit—and think about not where IT and cybersecurity have been, but where they are going. Where will the NSTAC "moonshot" take the nation and what will emerge along the expected trajectory. Some of today's emergent practices will be tomorrow's best practices. This is an opportunity to invest in those emergent practices. In addition, IT modernization investments should reflect an appreciation for the flexibility that will be needed to incorporate future innovative technologies and practices that will arrive during the life-cycle of the IT investments.

Enterprise email consolidation is an example of an IT modernization opportunity that could tremendously advance the efficiency of a commodity IT service while introducing levels of cybersecurity previously unknown across the federal enterprise. Email consolidation is an expected modernization effort. Each of the "Report to the President on IT Modernization" and the "Federal Cybersecurity Risk Determination Report and Action Plan" call for it across agencies. The IT modernization report argues that deploying cloud-based, enterprise email solutions "minimizes exposure of one of the most prominent cyberattack methods in modern society. Targeted, email-based spear phishing attacks using malicious attachments and links are the primary attack vector for compromising individuals and organizations."[13] The risk report similarly notes that "[e]mail, by way of phishing attacks, remains one of the most common attack vectors across both government and industry."[14] In fact, the U.S. Department of Energy received its award from the WCF for $15 million to support email platform consolidation within a single cloud service.[15]

This observation also is supported by other reports, such as Verizon's 2018 Data Breach Investigations Report, which notes that in Verizon's breach dataset detected malware arrives via email attachment or link 92.4% of the time.[16] This is consistent with a Cybersecurity Insiders' 2017 ransomware report, which observed that 73% of ransomware infections result from opening email attachments.[17] Putting this in context for the federal civilian government, the 23 CFO Act civilian agencies house 2.2 million email inboxes while the non-CFO Act agencies offer "hundreds of thousands of additional inboxes across 100+ small agencies."[18] Thus, the federal government finds itself with a large attack surface, spread across a distributed non-standard set of enterprise implementations and facing a highly prevalent threat vector specifically designed for that attack surface.

---

12 OMB, "Federal Cybersecurity Risk Determination Report and Action Plan", pp. 6-7.
13 American Technology Council, "Report to the President on Federal IT Modernization" (Dec. 13, 2017), pp. 24-25.
14 OMB, "Federal Cybersecurity Risk Determination Report and Action Plan", p. 13.
15 Accessed June 26, 2018 at: < https://www.nextgov.com/it-modernization/2018/06/first-modernization-fund-winners-offer-cheat-sheet-future-pitches/149007/>.
16 Verizon, "2018 Data Breach Investigations Report". Available at: <https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf>.
17 Cybersecurity Insiders, "Ransomware: 2017 Report" (sponsored by AlienVault). Available at: <https://learn.alienvault.com/c/2017-ransomware-report?utm_internal=ransomwarelookbook&x=t0YTjn&xs=15156>.
18 OMB, "Federal Cybersecurity Risk Determination Report and Action Plan", p. 13.

This is an opportune time to revisit best practices surrounding email security while building better security technology into enterprise email solutions. In 2017, DHS issued Binding Operational Directive (BOD) 18-01, "Enhance Email and Web Security", which required federal agencies to implement STARTTLS and a set of email authentication rules and policies, such as Domain-based Message Authentication, Reporting & Conformance, to hinder passive man-in-the-middle attacks and spoofed emails, respectively. Consolidated enterprise email services will reduce the individual instantiations of BOD 18-01 required to achieve compliance with the directive, which has been difficult for some agencies. However, these practices focus on improved security around the email infrastructure. The government also should examine its security practices focused on email content.

Generally, email attachments are scanned by traditional, signature-based antivirus solutions at the email gateway and upon execution at enterprise endpoints. Innovations have added heuristic-based antivirus solutions and sandboxing opportunities. A large organization is likely to maintain multiple security solutions in its email security stack. These solutions offer evolving ways to detect and prevent malware. Such organizations' success is largely based on prior experience—a combination of previously seen malicious files, malicious behaviors, suspect behaviors, and other attributes of prior attacks, or on hope, luck, and waiting for others to be victimized. Yet email-based malware continues to effectively compromise individuals and organizations. Increasingly, it is used as a pivot-point from which so-called "file-less" malware can be introduced into an enterprise, which presents its own detection and prevention challenges.

Go…Running Smarter to become Faster

Considering the continued success malicious actors experience using phishing emails loaded with malicious attachments, one can only conclude that while detection is necessary for effective cybersecurity, it is not sufficient. For too long, the cybersecurity community has been trying to solve an increasingly intractable problem—identifying and stopping malicious file attachments before they infect an endpoint or network. Yet, automated assembly-line malware generation on an industrial scale, coupled with malware that can be made sandbox-aware or at least sandbox-evading, will continue to defeat detection approaches far too often. The end goal of preventing malicious files from infecting an enterprise remains sound, but it requires solving a simpler problem. Instead of detecting and preventing "known-bad" files, enterprise email security must incorporate technology to simply look for, generate and pass "known-good" files.

Generating and passing "known-good" files can be achieved using deep-file inspection, remediation and sanitization technology (d-FIRST™), which is already available in the cybersecurity marketplace. Glasswall FileTrust™ Advanced Threat Protection is just such a technology. In an average of 200 milliseconds, it will compare a file to that file type's standard or specification (e.g., ISO 10918 for JPEG, ISO 32000 for a PDF file or [insert a Microsoft Office protocol), regenerate the file in accordance with that specification, and pass the file forward. During the regeneration process, Glasswall FileTrust™ performs two sets of actions. First, it remediates structural deviations from the file type specification. This includes fixing byte-level anomalies, which may be intentionally or unintentionally introduced into the file, but can create unwanted consequences. Second, it sanitizes functional aspects of the file based on an enterprise's security policies. For example, it can remove extensible attributes, such as macros, JavaScript, embedded files and metadata. Sanitization can be applied differently depending on user groups and their business needs.

The d-FIRST™ approach is a departure from traditional security techniques. All files are subjected to it instead of only acting on files that match a signature or heuristic pattern. The results, however, fill a gap in traditional architectures. For instance, Glasswall Solutions tested 6,000 known and unknown malicious files with a global defense contractor. Initially, only an antivirus solution was deployed. Of the 6,000 malicious files, 3,592 of the files were detected by the antivirus solution—a 40.13% failure rate. Subsequently, a heuristic layer was added by the systems integrator, which reduced the failure rate to 35.58%. Finally, Glasswall FileTrust™ was inserted in place of the signature- and heuristics-based solutions. Each of the 6,000 files was effectively remediated and sanitized.

In an operational example, a Glasswall Solutions customer received 347 million emails over a six-month period, including Microsoft Office, PDF and image files. Four layers of defense were applied to the files, including next generation firewalls, anti-spam and anti-phishing filters, antivirus solutions and a heuristics filter. Fifty-five million of the original files were

processed and allowed to pass to Glasswall FileTrust™, the company's final line of defense prior to the email server. The multiple security layers failed to prevent 171 malicious files, almost an average of one file per day. According to the customer, Glasswall FileTrust™ neutralized the threats with no impact to the end-user experience. Glasswall Solutions began querying well-known malware repositories with the hashes of the original 171 malicious files. In some cases, the malware was known to the antivirus community, but the traditional solutions did not prevent those files. In other instances, not only did Glasswall FileTrust™ protect the customer on day-zero, but it took up to three, seven and even 30 days for the antivirus community to indicate awareness of the malicious files. Of course, with the d-FIRST™ approach this is to be expected. By subjecting all files to the security solution, previously unknown malware will be rendered inert. Customers are not only protected by Glasswall FileTrust™ on day-zero, but they have access to personalized threat intelligence as these are files often specifically directed towards them.

Not surprisingly, this approach is rarely if ever identified as a practice within standards and guidelines issued by government agencies and international standards development organizations. There is a robust set of standards and best practices related to malware. For example, the U.S. National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" (NIST CSF) highlights several standards, guidelines and practices applicable to the detection of malicious code and unauthorized mobile code. Among those are provisions of NIST's own NIST SP 800-53 Rev. 4 and other guidance including around mobile code and malware incident response. The guidance generally focuses on signature-based antivirus.

For example, the NIST SP 800-53 Rev. 4 SI-3 (Malicious Code Protection) control focuses on employing malicious code protections at ingress and egress points to detect and eliminate malicious code, updating those protections when new releases are available, configuring them to perform periodic and real-time scans of files from external sources, and blocking, quarantining or alerting when malicious code is detected.[19] The associated supplemental guidance recognizes that malicious code can be introduced through email and email attachments. SI-3 further offers that protections "include, for example, anti-virus signature definitions and reputation-based technologies" as well heuristic-based solutions.[20] Similarly, NIST SP 800-28 Ver. 2, "Guidelines on Active Content and Mobile Code", suggests a series of policy and configuration controls as well as technical safeguards such as filters. However, filters are dependent on some degree of prior knowledge regarding malicious content. As articulated by NIST:

> Many enterprise firewalls can filter email and Web pages for well-known file extensions and block them at the point of entry, following configured screening rules. More sophisticated ingress gateway filters can block or disable malicious code conveyed as active content. Desktop antivirus software has become increasingly capable of detecting active content having a malicious code signature. Client applications such as browsers, email, and word processors can also be configured to disable or ignore some forms of mobile code.[21]

NIST also recognizes the limitations of these approaches:

> While firewalls, antivirus software, and intrusion detection tools provide useful safeguards, they are not foolproof. Constructing a program to detect with certainty the presence or absence of harmful code within arbitrary programs or protocol is impossible. Moreover, a variety of techniques exists for deception such as mutation, segmentation, and disguise via extended character set encoding. Thus, filtering tools are faced with the prospect of diminishing returns – greater investments are needed for small increases in effectiveness. Despite services to refresh protection software with signatures of known exploits, and cascaded defense-in-depth measures, apart from total isolation there is no guarantee that something harmful cannot get through.[22]

---

19 Id., p. F-217.
20 Id., p. F-218.
21 NIST SP 800-28 Ver. 2, p. 5-8.
22 Id.

As a report by PhishMe, Inc. notes, "[f]or the past three years, one of the most commonly-used means for delivering malware by phishing email has been using macro-enabled Microsoft Office documents" as well as using OLE object abuse and PDF files that, upon execution, creates a Word document that incorporate a macro script.[23] Simply implementing configuration policies that preclude the use of macros is insufficient. User awareness training can assist in reducing the prevalence of phishing attachments and URL links clicked by email recipients, but a defense-in-depth strategy suggests that an organization should not rely on training alone. In addition, it suggests that organizations need to carefully assess blacklists, reputation services and similar mechanisms, each of which is dependent on some level of prior knowledge regarding malware, before deploying them to minimize false-positives and false-negatives.

Although the PhishMe report articulates the benefits of signature and heuristic-based malware protection, it also notes the limitations of those solutions. Similarly, AV Comparatives observes that some antivirus "products may block files based solely on their prevalence, i.e. if a vendor does not have any data for a particular file, their product may treat it as a threat. This of course helps to block many malicious files, but at the same time it can lead to higher false-alarm rates by blocking clean files which currently have zero or very low prevalence in the user base of the particular vendor."[24]

Over time, new NIST guidance and revisions to prior publications have recognized the need to move beyond reliance on signatures alone, and heuristic-based solutions have been added to the group of non-signature based approaches that can be implemented as part of a security control. The absence of specific reference to d-FIRST™ solutions within the NIST body of work is not surprising as the technology is relatively new. Despite this, the use of d-FIRST™ solutions must quickly become recognized as an emerging practice. The results Glasswall Solutions has seen with its customers suggests the security benefits afforded by its Glasswall FileTrust™ offering provide a level of protection against malicious files far beyond that afforded by current, common email security architectures. Fortunately, the structure of NIST special publications anticipates incorporating new practices as they emerge. In fact, the draft of NIST SP 800-53 Rev. 5 further opens the door to an increased recognition and use of non-signature based protection at ingress and egress points. However, the revisions largely increase the focus on heuristic and artificial intelligence-driven solutions. IT modernization and improved cybersecurity risk management will benefit from incorporating d-FIRST™ solutions.

Coupled with initiatives to centralize enterprise email, d-FIRST™ solutions will be easily incorporated into the broader set of email security tools. Furthermore, d-FIRST™ makes sense in the context of another initiative highlighted in the risk report to the President. Agencies are expected to standardize their software and applications. "OMB and the General Services Administration (GSA) will work with agencies to move to standard configurations or versions through shared services and new government-wide marketplaces."[25] The report observes that this will "augment the software application whitelisting capability that DHS is providing to agencies in [Continuous Diagnostics and Mitigation] Phase 1," and that it is "critical to allocating resources effectively during the acquisition process and, more broadly, in securing the Federal environment as a whole."[26] Yet, what is the value of whitelisting applications, such as the Microsoft Office suite, if the files opened by those applications are themselves malicious? The use of d-FIRST™ solutions alongside whitelisted applications dramatically reduces the unknown attributes of an enterprise—the applications running on the network are known and the files they handle are equally "known" based on reference to their file type standards and specifications.

---

23 PhishMe, Inc., "Malware Review, Q2 2017", pp. 7-8 (accessed at www.phishme.com).
24 AV Comparatives, "Whole Product Dynamic 'Real-World' Protection Test", dated December 12, 2017 (accessed at www.av-comparatives.org).
25 OMB, "Federal Cybersecurity Risk Determination Report and Action Plan", p. 14.
26 Id.

Conclusion

The U.S. government's effort to modernize its IT infrastructure while improving its risk-based approach to cybersecurity is to be commended. What began as a policy initiative with an executive order has produced a set of actionable implementation items. Supported by legislative authorizations and appropriations, the effort is positioned for success.

However, it is during this period of project execution that those implementing the policy cannot lose sight of the big picture. Yes, technology investments are important, but they cannot be undertaken in a vacuum. Technology acquisition decisions need to contemplate related governance, process and staffing needs. Similarly, investments should consider standards, best practices and emergent practices. To the extent practicable, IT acquisitions and investments in security controls must be flexible so that they can incorporate current and future innovative technologies and processes. Perhaps one of the best-kept secrets in cybersecurity, Glasswall FileTrust™ Advanced Technology Protection is just such an innovative approach to security, which will quickly move from an emergent practice to a best practice. It behoves those interested in IT modernization and investing for the future to consider how to best integrate the d-FIRST™ approach into a consolidated, cloud-based enterprise email commodity IT service offering.

GLASSWALL