FROM THE INSIDE OUT: CREATING A HOLISTIC CYBERSECURITY STRATEGY FOR GOVERNMENT

INDUSTRY PERSPECTIVE

Hewlett Packard Enterprise

EXECUTIVE SUMMARY

Complexity and a lack of strategic planning undermine our government's cybersecurity. The government does have the ability to protect our data and IT resources; what is needed is a strategic, risk-based program that prioritizes its most valuable assets.

Today, government's IT infrastructure is under increasing pressure from a variety of adversaries with a number of objectives, ranging from individual and organized criminals seeking financial gain to nation states seeking political and military advantages to activists and terrorists seeking to undermine basic values.

The result has been a deluge of attacks that have harmed agencies, put government employees and other citizens at risk and damaged confidence in our democratic processes. Breaches of the Internal Revenue Service and the Office of Personnel Management have exposed personal information of millions of individuals. Leaked information stolen from political party officials has been used in attempts to sway a presidential election, and attempts have been made to access state voter registration databases.

This situation does not have to continue. There exists the capability to protect the nation's data and IT resources. But something is missing: a strategic, risk-based cybersecurity program that prioritizes the nation's applications and data. Implementing it, however, means overcoming some particular challenges.

To help you understand why a holistic and strategic program is necessary for the public sector today, and how to actually achieve it, GovLoop spoke with **Earl Matthews**, Vice President, Enterprise Security Solutions Hewlett Packard Enterprise Services, U.S. Public Sector. Matthews is a highly decorated, award-winning retired U.S. Air Force Major General with a successful career influencing the development and application of cybersecurity and information management technology.

> "Getting cybersecurity right is like the space race. Today, cybercrime actually exceeds the drug trade. The United States needs a national program to address this critical issue."
>
> **Earl Matthews,** Vice President, Enterprise Security Systems Hewlett Packard Enterprise Services, U.S. Public Sector

WHY IS GOOD CYBERSECURITY SO HARD?

The Government Accountability Office first listed federal cybersecurity as a high-risk issue in 1990, and it has remained on the list for nearly three decades. So why is it still so difficult to protect information systems and the data they contain?

Part of the reason is that cybersecurity threats to every enterprise are evolving. Lone hackers have been replaced by highly motivated, well-resourced organizations supported by a black market that commercializes the latest exploits, offers botnets as commodities and provides a marketplace for stolen data. However, the primary reason that defense is so difficult can be summed up in one word: complexity.

The architecture of most government IT enterprises is too complex. Networks have been knitted together without an overall plan or goal, with new technology being added while legacy technology remains in place. The result is that senior leaders often have poor visibility into the enterprise and an inadequate understanding of the systems they are responsible for securing and how they interact. According to Ponemon's 2016 Cost of Cyber Crime Study, 81 percent of cybersecurity budgets are spent on 10 to 25 percent of vulnerabilities, leaving a large window of opportunity for adversaries.

Modernizing and rationalizing the IT infrastructure would provide a higher return on investment. Security vendors often simply respond with new products and tools to address each cyber threat as it emerges, and government responds by buying the newest products. This produces still more complexity, with too many tools from too many vendors that cannot be effectively implemented, monitored and maintained.

"Most organizations have over sixty-six security products that they are using to protect their environment," Matthews explained. "Industry and organizations chase the next shiny object instead of forming a comprehensive roadmap or security plan. As a result, you have so many products, you don't have enough training to go with the people tasked with implementing these tools. This leads to too many privileged users having access to the network."

With no security roadmap to guide federal administrators, new products bought by agencies sometimes remain in the box, unused. Furthermore, agencies often do not have the skilled workforce to deploy these tools nor the time or budget for training so that they can be effectively used. Resources continue to be used for putting out fires rather than learning how to prevent them.

A Risk-Based Focus

Cybersecurity effort goes primarily into protecting the enterprise from the outside in — blocking attacks as they come into the systems from the outside. While there is logic to this approach, it ultimately is a losing strategy in such complex environments that can leave the most valuable assets vulnerable. A risk-based program focused on the most valuable and vulnerable assets would use finite resources to defend those assets that are most likely to be targeted and whose compromise would have the greatest impact.

"We need to take a different approach -- look at it from the inside out," Matthews said. "When you're looking at cybersecurity from the outside in, then you're just trying to block. But if you approach it from the inside out, then you can think about it from the angle of, what are my most critical apps and data? So let's look at a risk-based strategy instead of a compliance-based one."

Most successful security breaches today target the application layer, and the intruders' ultimate goal is the data.

> "Industry and organizations chase the next shiny object instead of forming a comprehensive roadmap or security plan. As a result, you have so many products, you don't have enough training to go with the people tasked with implementing these tools."
>
> **Earl Matthews,** Vice President, Enterprise Security Systems Hewlett Packard Enterprise Services, U.S. Public Sector

PROTECT FROM THE INSIDE OUT

Despite the continuing drumbeat of bad news, government is not ignoring cybersecurity.

In fact, the administration has initiated a number of cybersecurity programs, including the National Action Plan, which created the position of Federal Chief Information Security Officer. In September, retired Air Force Brig. Gen. Gregory J. Touhill was named the first Federal CISO to drive cybersecurity policy, planning and implementation across government.

These and other initiatives, including the IT Modernization Fund and the Cybersecurity Strategy and Implementation Plan, have been positive steps toward improving federal cybersecurity. But although the steps have been a move in the right direction, they have not been enough to create a comprehensive cybersecurity posture in government that is capable of proactively protecting the nation's most valuable assets. Agencies still are focused more on blocking intrusions from the outside rather than risk-based protection of data and applications. Budget appropriations for cybersecurity do not reflect the challenges being faced by agencies, and there is too little accountability. Although agency heads can be called before Congress and even risk losing their jobs in the wake of particularly damaging breaches, there is little day-to-day accountability for establishing and maintaining cybersecurity programs.

> The original Federal Information Security Management Act of 2002 (updated as the Federal Information Security Modernization Act of 2014) is an attempt to create coherent cybersecurity policies across government, and the National Institute of Standards and Technology (NIST) has produced an extensive library of cybersecurity guidance for implementing FISMA.

Government is in the process of a fundamental shift in IT under the cloud computing strategy. Under this cloud-first policy, agencies are taking advantage of the scale, economy and flexibility of cloud computing to speed up IT modernization and improve delivery of government services. Whether the cloud platforms are private, public or hybrid, this paradigm shift offers a chance for agencies to implement the strategic capabilities needed for a comprehensive cybersecurity program.

"We need to think about what is the interaction among the application, the data, and the user," Matthews said. "There are things we can do to shore up legacy environment. You need to be strategic about it in the following ways."

Assuring Application Security

Applications are the primary target for hackers, with more than 70 percent of successful breaches directed at the application layer. A complete cybersecurity posture requires applications that are developed with security built in and regularly assessed to ensure that they remain secure.

Vulnerabilities become embedded early in the application development lifecycle. Finding and fixing them early in the lifecycle dramatically reduces the cost of these fixes. Reactive measures such as security code scanning and penetration testing are ineffective or inefficient in fixing these flaws.

HPE's Comprehensive Applications Threat Analysis (CATA) service is a proactive way to avoid these defects from the start of the lifecycle. HPE developed this vulnerability assessment service to reduce the number of undiscovered security defects in their own software, and CATA can be applied at any point in the application lifecycle, from development to production. Conventional application development methods discover a small fraction of vulnerabilities before software is released to production. To discover vulnerabilities earlier, CATA offers:

- ***Security Requirements Gap Analysis***, to identify requirements of common industry and government standards that have not been adequately addressed.
- ***Architecture and Design Threat Analysis***, an architecture-level review of the security properties of underlying components to enable resilient designs.

CATA also functions as an independent validation and verification of security requirements and architectural security resilience for any applications development project. The result is an application that is secure by design. Leveraging the expertise of HPE security consultants can minimize the costs of identifying and fixing problems after the fact, providing a faster return on your investment.

Good Cyber Hygiene

The standard for federal cybersecurity has moved from periodic assessment of static security controls to continuous monitoring. The Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program supports continuous monitoring by making available a suite of off-the-shelf products to give real-time visibility into networks and systems. NIST's Risk Management Framework provides a risk-based approach to managing organizational risk for critical infrastructure. Properly implemented, these programs can help agencies identify vulnerabilities and mitigate risks on an ongoing basis.

HPE has created a unique shared services platform that combines security information produced by the wide variety of products used in CDM and the Risk Management Framework with the organizations' mission asset information. This provides a holistic view of the status of basic security controls. HPE was also the first to reach the required DHS operational milestone.

This shared service is aimed at smaller agencies that might not have the technical resources and expertise to perform critical security work themselves. Information from endpoints, hosts and local networks is securely sent to the service to perform complex aggregation, correlation, analysis and risk-scoring in a multitenant environment. This can help agencies get the most from their current security investments. Data from a variety of sources and tools is normalized to provide a single, authoritative point for accessing data. Cyber incidents and affected assets are correlated with specific missions and mission assets. This allows organizations to respond not only to the cyber threat itself, but also to the mission, if necessary, to ensure it is protected.

The HPE solution provides the ability to manage by risk, respond to incidents and apply appropriate courses of action in the mission space.

Stay Ahead With Managed Services

Protecting IT resources is critical for every agency, but cybersecurity is not a core competency for most. Achieving the real-time visibility and performing the monitoring and analysis needed for effective cybersecurity is often a challenge beyond agencies' resources and expertise. Managed services provided by experienced professionals can help agencies meet cybersecurity requirements without the capital expenditures and manpower costs of in-house operations.

HPE is a leader in managed security services. Agencies can benefit from HPE's holistic expertise, provided from its U.S. Public Sector Security Operations Center (SOC) in Herndon, Va. and Boise, ID, freeing agencies to focus on their missions.

"The biggest benefit is the global threat intelligence that HPE provides," Matthews said. "We are ahead of the threat when it comes, because we can leverage what we see on other people's network and when combined with our partner FireEye's capability for Advanced Persistent Threat is very powerful.

The HPE SOC supports the latest technologies to provide 24-7 monitoring year-round. Agencies benefit from the scale of a managed service without the expense. Experienced security professionals — most with government security clearances — also provide incident response, incident handling and mitigation. Capabilities include intrusion detection and prevention, firewall support, sensor monitoring, relational analysis, analytical integration and exposure mitigation. HPE's customers also benefit from its global threat intelligence, gleaned from monitored networks worldwide — a capability that in-house operations do not have the scale to provide.

In a competitive environment for skilled cybersecurity workers, HPE's managed service gives agencies the benefit of an experienced professional workforce without the expense of hiring, training and retaining personnel, often an agency's greatest cybersecurity challenge and expense.

PUTTING CYBERSECURITY TO WORK

HPE has been awarded one of the 17 blanket purchase agreements for the Dept. of Homeland Security's Continuous Diagnostics and Mitigation (CDM) program, a dynamic approach to bolstering the cybersecurity of government networks and systems. CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritizes these risks based upon potential impacts, and enables cybersecurity personnel to mitigate the most significant problems first. The program enables government entities to expand their continuous diagnostic capabilities by increasing their network sensor capacity, automating sensor collections, and prioritizing risk alerts. The HPE implementation of CDM has demonstrated its thoroughness and vision and allows agencies to get up and running more quickly to meet all aspects of cyberthreats through expert knowledge in integrating the various tools in an agency's environment.

THE FUTURE OF CYBERSECURITY

The history of cybersecurity has been reactive, with enterprises and security vendors struggling to catch up to threats and vulnerabilities introduced by rapid changes in technology. Technology will continue to change rapidly, but this does not mean that cybersecurity must remain a losing race to keep up with threats.

"We must create an architecture that is resilient enough that agencies can still continue their business and serve citizens," Matthews concluded. "It's a little bit like installing brakes on a car. Brakes were not invented to stop a car. They were invented so you could drive faster, safer, slow down when you might need to, and come to a complete stop if necessary."

The key to moving ahead of the threat curve lies in changing the security culture by raising awareness, better data security and security analytics. A strong, risk-based national program that prioritizes assets as well as threats and vulnerabilities can help the U.S. government defeat adversaries by letting it protect what is valuable — data and applications — rather than reacting to every incident. This shift will help cybersecurity become an enabler of functionality rather than a cumbersome afterthought.

About HPE

Hewlett Packard Enterprise creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. As the world's largest technology company, HPE brings together a portfolio that spans printing, personal computing, software, services and IT infrastructure to solve client problems.

www.hpe.com | www.hpe.com/gov/transformation | @HPE

About GovLoop

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 250,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

1152 15th Street NW, Suite 800 Washington, DC 20005
Phone: (202) 407-7421 | Fax: (202) 407-7501
www.govloop.com
@GovLoop