Market Connections
Research you can act on.

Cyber Security and Transformational Technologies

Keeping Systems and Data Safe

A WHITE PAPER PRESENTED BY:

The Lockheed Martin Cyber Security Alliance

November 2012

LM CYBER SECURITY™ ALLIANCE

LOCKHEED MARTIN

We never forget who we're working for®

PREPARED BY:

MARKET CONNECTIONS, INC. 14555 AVION PARKWAY, SUITE 125 | CHANTILLY, VA 20151

T703.378.2025 | F703.378.2318 |WWW.MARKETCONNECTIONSINC.COM

CYBER SECURITY AND TRANSFORMATIONAL TECHNOLOGIES

Keeping Systems and Data Safe

Since 2010, Lockheed Martin and its Cyber Security Alliance Partners have commissioned annual research studies to measure awareness, attitudes, level of comfort, and trust with cyber security and emerging technologies. The third annual study focuses on how government IT professionals are applying transformational technologies to address cyber threats, delivery of services to an increasingly digital and mobile citizenry, and tackling complex problems by tapping into vast stores of data.

EXECUTIVE SUMMARY

Federal IT professionals are facing an increasingly complex landscape of rapidly changing technology, presidential directives that affect priorities, constrained resources, and escalating cyber threats, according to the Lockheed Martin Cyber Security Alliance survey on IT issues conducted by Market Connections, Inc.

The Obama Administration's "Big Data Research and Development Initiative," introduced in March 2012, calls on agencies to find ways to improve their extraction of knowledge and insights from large and complex collections of digital data. These insights can be applied to hugely complex problems—setting the stage for the White House's release of its Digital Government Strategy (DGS) in May. Just as IT professionals shaped their priorities to integrate the Obama Administration's directive on cloud computing last year, now they are wrestling with the rapid expansion of mobility as a strategy and an objective.

Hovering over the creation of a new digital government are cyber threats. If the federal government hopes to create a new digital relationship between citizens and agencies, then cyber security becomes more critical than ever. To support both e-government and e-commerce, the National Institute of Standards and Technology (NIST) in February established its National Cyber Security Center of Excellence, working with the State of Maryland and Montgomery County, Md.

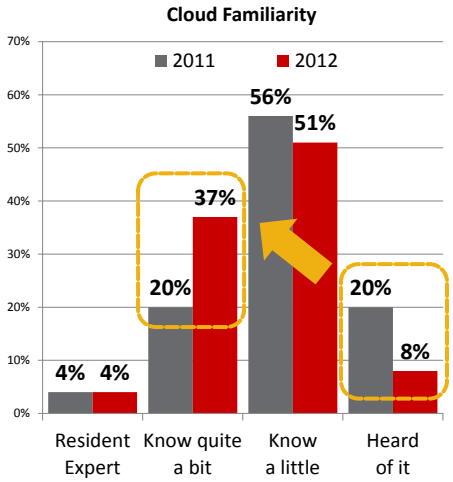
"Of the three—cloud computing, big data and mobility—mobile devices are possibly the most transformational… being able to walk around anywhere with my hand-held device and to access information from some service provider. To me, it's been a life-transforming thing. And I'm imagining what it would be like to broaden the reach of those devices."

IT SPECIALIST, FEDERAL CIVILIAN AGENCY

The Emergence of Transformational Technologies

In the 2011 Lockheed Martin Cyber Security Alliance Study, many IT professionals in the government expressed concerns about cyber security in the cloud. This was in part because, while they were eager to embrace the potential cost savings, flexibility, and ability to create new collaborative models, they did not know enough about the workings of security under different models—public, private, and hybrid clouds—to protect sensitive information.

Today, their knowledge of cloud computing has expanded. Some 37 percent of government IT professionals responding to this year's study "know quite a bit" about the subject today, almost double last year's 20 percent, and another 51 percent "know a little bit."

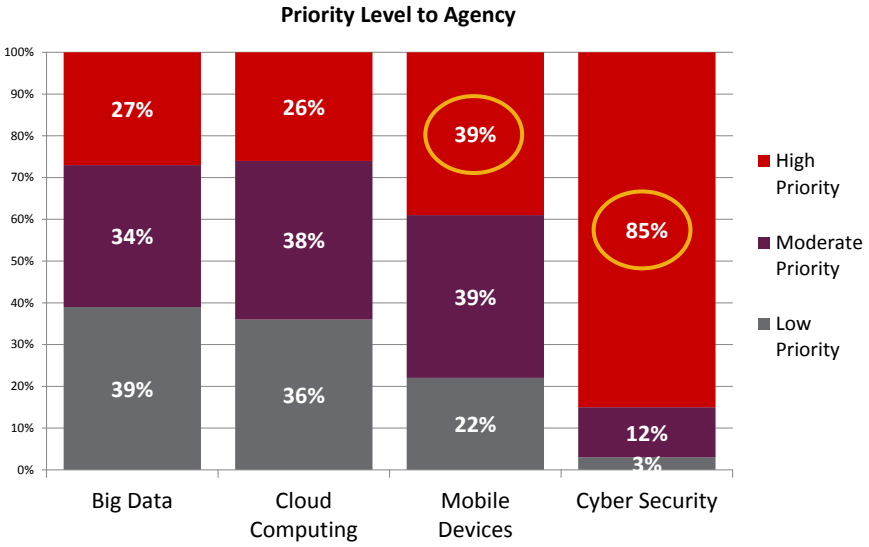


Despite that, their priorities have shifted. The DGS, with its call for services to be delivered to citizens in digital mode, lifted mobility—39 percent of government IT professionals see mobile computing as a high priority, while 27 percent consider big data a high priority, followed by cloud computing at 26 percent.

"I think there's an awareness that the amount of resources required to adequately address cyber security threats are known to be very hard to look at in the current austerity environment. But, it will continue to be a high priority."

CHIEF, INFORMATION MANAGEMENT, DOD

Trumping them all, though, is cyber security. Some 85 percent of government IT professionals rate this as a high priority, perhaps because they recognize that each of these—cloud computing, mobile computing, and big data—pose security risks and challenges, some in common across all, and some unique to each sphere.



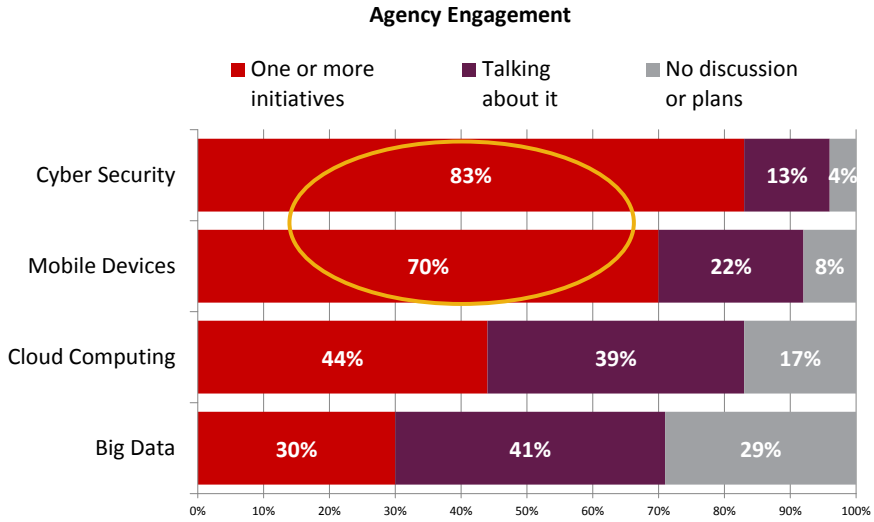
These priorities are reflected in actions taken. About 83 percent of IT professionals indicate their agency has one or more major initiatives underway in cyber security, while 70 percent have one or more mobile computing initiatives in progress. One or more cloud initiatives are being undertaken by 44 percent of government IT professionals; of course, cloud projects have been underway for at least two years, so this should not be seen as a lower priority. About 30 percent of surveyed IT professionals said they have one or more big data projects underway or in the works. As the newest addition to federal IT to-do lists—and the most speculative—this may not be surprising.

Cloud Computing Models Becoming More Diverse

The ability of cloud computing to support more than one approach to provide the combination of features, security, and scalability means that there are several different models that are gaining traction within the government.

"There'll be a cost and time associated with migration to cloud, so if in the near term there are resources associated with the move that we can't produce based on the outcome of sequestration and those sorts of things that are hanging out there, that would obviously freeze us in place, despite any efficiencies."

CHIEF, INFORMATION MANAGEMENT, DOD



Federal community clouds—a model where two or more agencies share a cloud—are anticipated to be used by 52 percent of IT professionals, while 42 percent expect to use private clouds dedicated to their agency or department. Using public clouds, such as Google's commercial offering, are expected by 16 percent of study participants. Hybrid clouds, which are comprised of some public areas and others which are private, are anticipated by 21 percent of government IT professionals.

"In some ways, I think there's an illusion that by hosting the information on your own network you're somehow safer."

IT SPECIALIST, FEDERAL CIVILIAN AGENCY

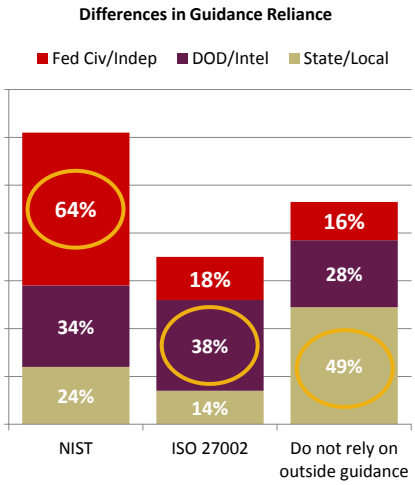
And this is subject to change and evolution. Percentages add up to more than 100 percent because agencies can, and do, use more than one cloud or type of cloud.

Cyber Security Awareness Rising in a Complex Environment

Greater dependence on IT systems to deliver services has increased government IT professionals' use of security resources—from NIST, ISO 27002, FedRAMP, Apps.gov, the Cyber Security Alliance, and others. There are distinct differences between federal civilian agencies, Defense Department/intelligence agencies, and state and local agencies.

NIST is used most by federal civilian agencies (64 percent of study participants); 34% of DOD/intelligence agency IT professionals use NIST guidance; while just 24 percent of state/local government IT decision makers said they use its resources.

ISO 27002, an information security standard published by the International Organization for Standardization and the International Electrotechnical Commission, provides best practice recommendations for information security management. This is used by more than a third of DOD/intelligence agency IT professionals (38 percent), while just 18 percent of federal civilian study participants and 14 percent of state/local agencies use it.



"With the policies in place now, I think we're 100 percent better than we were five years ago."

PROGRAM ANALYST, DOD

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program administered by the General Services Administration to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. It is most used by federal civilian agencies (23 percent); just 15 percent of DOD/intelligence agency IT decision makers said they use it, and none of the state/local agency study participants. This may be consistent with the use of cloud computing, since DOD and intelligence agencies have been slower to move to the cloud.

Apps.gov, another service of the GSA, is a cloud computing portal that serves as a storefront for approved cloud computing applications. It is not as popular a source for cyber security guidance; just 16 percent of federal civilian agency and 13 percent of DOD/intelligence agency IT professionals said they use it, and just 5 percent of state/local agency study participants.

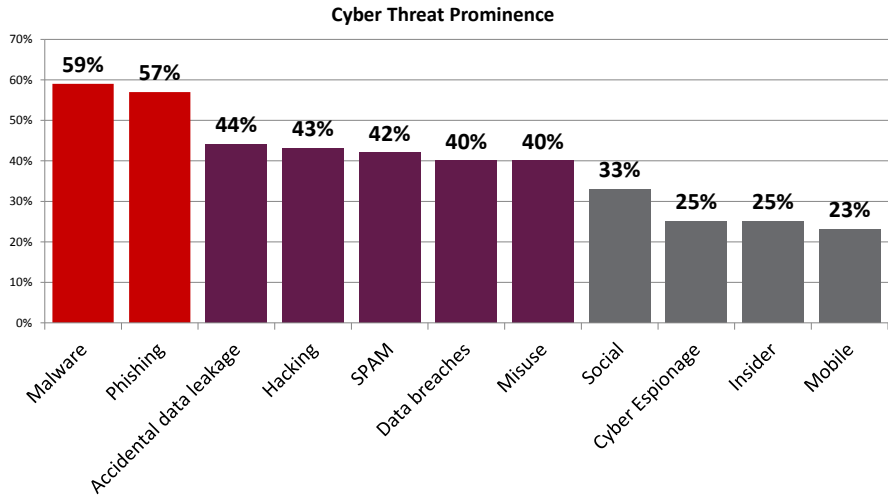
The Cyber Security Alliance (CSA) is a source of security guidance for 8 percent of DOD/intelligence agencies, 6 percent of federal civilian agencies, and 3 percent of state/local agencies, based on responses.

It may raise flags that 26 percent of study participants overall—28 percent of DOD/intelligence agencies, 16 percent of federal civilian agencies, and 49 percent of state/local agencies—say they do not rely on guidance from outside their organizations.

Where Do Threats Come From—and Are Agencies Ready?

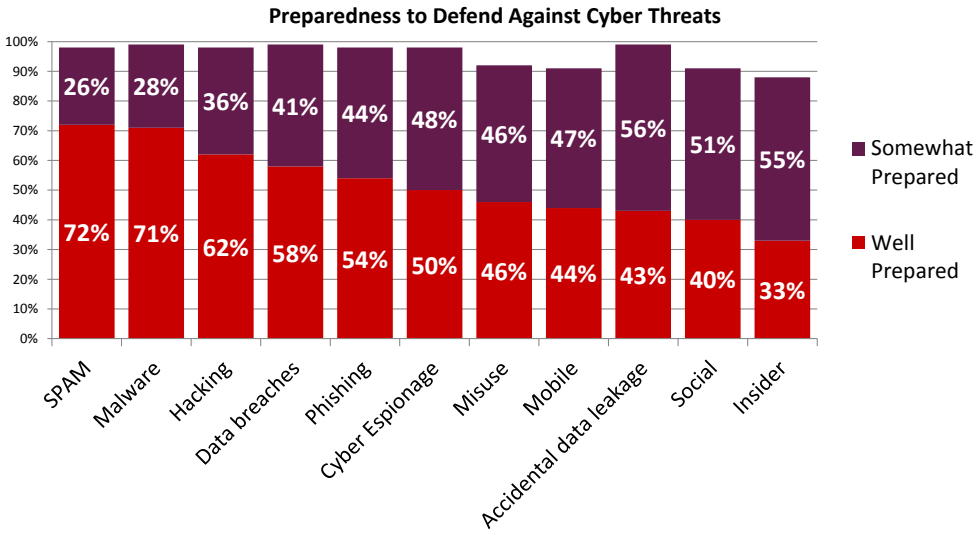
The cyber threat profile is multi-faceted. It includes malware, phishing, hacking, spam, social engineering, cyber espionage, mobile, and insider threats—and that does not include human mistakes such as accidental data leaks or misuse. Some of these threats, such as hacking and malware, have been around as long as the Internet; others, specifically general user threats, have spread as individuals have adopted new technologies faster than IT professionals have been able to keep up with securing them.

Malware is the most prolific threat, identified by 59 percent of surveyed government IT professionals, followed by phishing (57 percent), accidental data leaks (44 percent), hacking (43 percent), spam (42 percent), misue (40 percent), data breaches (40 percent), social engineering (33 percent), insider threats (25 percent), cyber espionage (25 percent), mobile threats (23 percent), errors (18 percent) and physical threats (17 percent).



The most common outside threats—malware, phishing, hacking, and spam — are also those for which study participants feel best prepared. Combining well prepared and somewhat prepared responses for these four categories all reach 95 percent or more, and the percentage considering themselves well prepared is larger than the share considering themselves somewhat prepared.

Significantly, DOD and intelligence agency IT professionals have the highest degree of confidence for several types of threats. For instance, 83 percent of these study participants said they were well prepared and the remaining 17 percent said they were somewhat prepared for malware.



Social engineering threats—tricking a targeted computer user into taking some action or divulging information—are more challenging to defend against. All study participants, regardless of their agency affiliation, are more likely to be just somewhat prepared (51 percent) rather than well prepared (40 percent). Insider threats (55 percent) and accidential data leaks (56 percent) also fall toward somewhat prepared, rather than well prepared (33 and 43 percent, respectively).

Mobile threats are the emerging vector. Just 44 percent of all study participants believe they are well prepared, while 47 percent say they are somewhat prepared. This is the threat category with the lowest combined readiness percentage, and reflects how quickly mobile computing is overtaking established guard mechanisms, techniques and education.

What IT Investments Are Agencies Making?

"For every federal agency to be running its own data center is not efficient. The perfect thing is to outsource."

IT SPECIALIST, FEDERAL CIVILIAN AGENCY

Just under three-quarters of government IT professionals (72 percent) say they already have spent a lot of money on cyber security. This is reflected in their spending and contracting plans—just 30 percent are planning investments in cyber security, 25 percent have contracts in place for cyber security, and just seven percent plan to engage a partner to help with cyber security transitions.

A little more than a third of study participants (36 percent) have already spent money on mobile computing and 38 percent have plans to make an investment. About one-quarter (23 percent) already have contracts with mobile service providers, while 14 percent plan to hire a partner.

Some 39 percent of government IT professionals report their agency is planning new investments in cloud computing, while 21 percent have already invested in cloud solutions. Despite these figures, only 19 percent say they have contracts with cloud providers, while 15 percent are planning to find a partner.

"If the government is doing its job better, the public is better served, whether that part of the government is focused on defense, or building road infrastructure. Efficiencies will do more with less ultimately."

CHIEF, INFORMATION MANAGEMENT, DOD

It is easy to tell that big data is new on the IT scene. Only 16 percent of study participants say their agency has spent money on a big data initiative, 20 percent say they are planning to spend on such an initiative, 14 percent have contracts in place, and just 10 percent are planning to seek partners. Perhaps because big data is so new, 20 percent of government IT professionals say they need to figure out an exit strategy for a big data initiative before implementation, while another 19 percent say there is no business case for making the investment.

CONCLUSIONS

Emerging technology benefits outweigh the challenges.

The majority of study participants agree that an integrated approach to implementing cloud computing, big data solutions, and mobile initiatives would greatly benefit their agency (63 percent) and contribute to a more economical and affordable approach to sharing and storing information (70 percent). An integrated solution would include complete coordination and optimization of all

segments of the implementation, including virtualization, network, computer/servers, storage, and applications, with security inherently built into each layer as well as around the entire architecture.

"I definitely think mobile is transformational, if we can get it in the hands of the right people and make it secure… If you can have a technology data system where you can sit outside a cave in Afghanistan and draw data from a mobile device without giving away your position or any sensitive information, that's pretty valuable."

PROGRAM ANALYST, DOD

Fiscal realities rule in the federal world, however. One federal government IT professional in an interview described current conditions as an "austerity environment." It is unlikely that many agencies will be in a position to pursue complementary programs that look to build an integrated solution that maximizes the potential of these technologies to change government. Agencies will be seeking partners who understand and accept the fiscal constraints, while building in the potential to integrate disparate projects to acquire greater capabilities.

These three technologies—cloud computing, mobility, and big data—present very different challenges to organizations. The promise of cloud computing, which—when implemented well—is effectively invisible to the vast majority of government employees, lies in cost savings, flexibility, and the ability to add capabilities without an overhaul of legacy systems.

Mobility, on the other hand, is enticing because it has the potential to radically change how government workers do their jobs. It can boost productivity while making a government job more attractive to younger workers used to being "plugged in" wherever they are. Almost seven out of 10 study participants (69 percent) believe that mobile device management is about security of the devices.

"[We should be] putting information in the hands of citizens, to do whatever they want with it. It is public information. The public bought it, they paid for it, and it can probably be used in all sorts of innovative ways we haven't even thought of yet."

IT SPECIALIST, FEDERAL CIVILIAN AGENCY

Of the three, big data might be considered the wild card. For those working on big data projects, their excitement is based on discovering previously unimagined solutions to some of the nation's most enduring problems. It also has the potential to inject an almost entrepreneurial spirit into the government, as both public and private sectors look to build new models of performance based on information that has been locked away in vast quantities of raw data.

For all three, providing comprehensive cyber security must be foundational. Three-quarters of government IT professionals believe that secure cloud computing is indeed possible and their agency is well equipped to deal with cyber threats. That may be correct—but it may also be a reflection on the fact that three-quarters of government IT professionals also say they already have made significant investments in cyber security, even though many have yet to adopt cloud computing, implement mobile technologies, or start on big data projects.

ABOUT THE STUDY

Market Connections, Inc. was commissioned to conduct a study for The Lockheed Martin's Cyber Security Alliance to measure attitudes, awareness, level of comfort, and trust with cyber security and emerging technologies.

The study comprised 203 participants from in-depth telephone interviews and an online survey among decision makers and influencers of IT security solutions and services, with some level of familiarity with their agency's cloud computing, cyber security, mobility, and big data initiatives. Study participants represent all branches of the federal government and military services, a few intelligence agencies, and some state and local government agencies.

ABOUT THE LOCKHEED MARTIN CYBER SECURITY ALLIANCE

The Lockheed Martin Cyber Security Alliance combines the strengths of market leading companies' solutions and integrates their best practices, hardware, software, and tools within a unique new research, development, and collaboration center called the NexGen Cyber Innovation and Technology Center. The alliance companies include: APC by Schneider Electric, ArcSight, CA, Cisco, Citrix, Dell, EMC Corporation and its RSA security division, HP, Intel, Juniper Networks, McAfee, Microsoft, NetApp, Symantec, Trustwave, Verizon, and VMware.

ABOUT LOCKHEED MARTIN CORPORATION

Headquartered in Bethesda, Md., Lockheed Martin is a global security and aerospace company that employs about 120,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration, and sustainment of advanced technology systems, products, and services. The Corporation's 2011 sales from continuing operations were $46.5 billion. For more information visit: www.lockheedmartin.com.

ABOUT MARKET CONNECTIONS, INC.

Market Connections delivers actionable intelligence and insights that enable improved business performance and positioning for leading business, government agencies, and trade associations. The custom market research firm is a sought-after authority on preferences, perceptions, and trends among government executives and the contractors who serve them, offering deep domain expertise in information technology and telecommunications; healthcare; and education. For more information visit: www.marketconnectionsinc.com.