THE STAND Cybersecurity

Q&A with Industry Leaders

Over the next five years, government will spend $55 billion on keeping mission critical systems and data safe from malicious threats. But even with this level of commitment, the vulnerabilities will remain – and potentially increase.

THE STAND: Cybersecurity goes beyond the basic products and services stories and poses tough questions about federal cybersecurity to thought leaders at key vendor organizations. From this exclusive Q&A, you'll learn where they really stand on the state of cybersecurity challenges facing federal agencies today – and what they plan to do about it.

NORTHROP GRUMMAN

symantec™

THE STAND Cybersecurity

Question 1

How does your company view the cybersecurity threat today and how do you see it changing over the next five years?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: In the 30 years we've been working in cybersecurity, the situation has never been more dangerous. The threat from nation-states has become more sophisticated and well-financed and our critical infrastructure has become more dependent on cyberspace.

Threats will be increasingly targeted at particular organizations, types of systems and services, even individuals. Today's cyber aggressors are going after valuable intellectual property, sensitive information, and money. In some cases, the threats start with espionage and become part of warfare campaigns. We saw this in the Russia-Georgia conflict in 2008. These types of cyber attacks will become more common. The targets will also become more diverse. In the past, PCs and computer networks were the most common targets. In the future, the target list will also include infrastructure networks like the power grid and transportation systems.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: As I see the kind of security threat today, there is so much more malware out in the environment. There is so much more expertise behind the top attack vectors than we have previously seen in many years leading up to this point. The sophistication behind the attack structures is also at a much higher level.

So from the cyber security perspective, there is not a matter of "can I go out and get access to a system? Can I break into a system and then go brag about it?" Today, the threat is against the information that we use on a day-to-day basis to get our jobs done, to ensure that our companies operate smoothly and our country is operating smoothly. You see a level of sophistication, much better funding behind the efforts, much more high-tech talent trying to steal data information from systems, whether it is for financial gain or political gain. I think that is going to be the model that we'll be seeing for the next several years.

THE STAND Cybersecurity

Question 2

What do you consider to be the federal government's single biggest challenge in cybersecurity?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: From our perspective, the single biggest challenge is that there are way too many breaches that everyone already knows how to defend against – they're just not doing it fast enough. One of our customers, John Streufert of the State Department, testified on Capitol Hill about his risk-based approach to spending money smarter and focusing on fixing this problem. It worked at State, and it's starting to get traction in other departments.

We also hear from our government customers that they don't have enough qualified people and resources to do the job. Industry and government need to partner to help build the next generation of qualified cyber professionals.

That's why programs such as CyberPatriot, in which Northrop Grumman is a Presenting Sponsor, the Collegiate Cyber Defense Competition, and other STEM-related programs are so important to engage students and spark their interest in pursuing this career path. Through these types of programs, we can take steps to fire up the "cyber defender" side of our youth. If we can't prove to them (in their own terms) that the "protecting the network" side is just as intriguing as the "hacking the network" side, we'll have a dearth of talent and fall miserably behind our enemies.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: I believe the biggest challenge is data protection. Data and information protection is the number one concern, not only within the federal government, but any organization. Specifically, in the federal government – whether it is classified information or not – information has to be controlled. It's also a matter of understanding how that information is being used, where it resides, who has access to it, who should have access to it and how many versions of that information are actually out in the environment. Then you must protect it. You can't just look at the content of information today. You must look at content, context, value and relevance of the data to be able to protect it effectively. We must remember that most of the attacks today are done to steal data.

Take into consideration a simple e-mail, with an attachment, that a person sends to 3 other people. Each of these 3 other people also have a PDA so they receive the same information on their computer and their PDA. Even without considering data back-up and the high probability of one of these people forwarding the information, there are 7 instances of the same information on endpoint devices from the origination of a single e-mail.

What would you consider to be your company's unique value proposition when it comes to cybersecurity in the federal space?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: We have clearly demonstrated our ability to integrate disparate networks of all levels of classification into an effectively managed cyber system, focused on the mission of the enterprise. We believe that you don't just secure a network. You must secure the whole enterprise: its data, information, communications channels, and mission. Our decades-long expertise in cybersecurity cuts across every sector: intelligence, defense, civil, commercial and state and local. This experience, plus our internal research and market-leading university research approach, is accelerating the rate at which we can apply our approaches to defend our customers' enterprises.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: Symantec's unique value proposition is that we view the data and information that we use and need everyday as real jewels that we must protect. Protection and management of the data and information greatly reduces risk. Well-managed systems reduce risk. We can't forget that we are actually in a data explosion model, so the impact only grows with more concern. It adds a higher level of burden into organizations to better manage the access to data. So really, whether the data is on an end point, a storage device or in transit, Symantec protects the data and the systems that support that data with a high level of management and security functionality.

What unique core competencies does your company bring to the table in this space?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

John Bordwine
Public Sector CTO
Symantec

Edward Swallow
Northrop Grumman Information Systems

A: Our people are our most valuable asset. We have an aggressive human capital plan in place and more than 1800 Certified Information Systems Security Professionals to provide the workforce to successfully address the challenge.

We do state-of-the-art research in both cyber offense and defense. Understanding the offense is critical to playing good defense. We have adapted our military command and control capabilities to manage the cyber enterprise, both for customers and ourselves. We built a robust cyber test range more than 10 years ago, and have used it to evaluate, deploy and adapt technologies to address rapidly changing threats. We've also developed automated and semi-automated means for determining the mission-level impact of cyber disruptions, enabling customers to make effective decisions in the face of both imminent and enduring cyber challenges.

We are the industry leader in doing cyber defense research on the Internet2 high performance national research network, as part of our broadly based advanced R&D program. We are leveraging our Northrop Grumman Cybersecurity Research Consortium to advance the state of the art in cyber threat detection and mitigation and the development of inherently robust architectures using IPv6 and advanced technologies. This is a unique partnership with three world-class universities – Carnegie Mellon, MIT, and Purdue. Together, we are working on a wide variety of research projects to extend our interactions with the cybersecurity research community and to produce important innovations that we can implement in large-scale cyberspace operations. We are also making major investments in our own independent research and development efforts, focusing in the areas of modeling, simulation, and situational awareness.

John Bordwine
Symantec

A: Symantec has one of – if not the largest – repositories of information on the threat landscape in the world. So we are inventing new ways to better utilize this information to reduce the risk posture of many network environments. Our core knowledge is that repository. Being one of the leading security companies of the world allows us to look at new ways to use information – and information as we collect it – to provide a better risk posture to our customers.

What, specifically can be done to increase the security of classified networks?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

John Bordwine
Public Sector CTO
Symantec

Edward Swallow
Northrop Grumman Information Systems

A: The major security issues on classified networks come from the inside and the lack of endpoint security. Strong asset management, knowing where your endpoints are, real-time network monitoring, and improved awareness training are all very important. Better controls over use of flash drives and other external devices being connected to the network would also improve protection from malware. Expanded use of thin clients will increase endpoint security by eliminating the ability to actively attach data carriage devices.

Investing in eDRM (electronic digital rights management) technology is the real key to data security. With eDRM, you define data use policy, e.g. who can do what, and for how long. It addresses issues of data at rest, data in transit, and data in use - an ultimate data security solution that takes network level attacks out of the picture.

John Bordwine
Symantec

A: The key item to keep in mind is that if a human being touches it, there are going to be risks. Risks are created when humans interact with data and information in the system. So you have to define the appropriate security policies that take into consideration all aspects of the environment. Due to the high level of importance within a classified network, technology should be in place to better define a predictive analysis model.

What are some emerging technologies or processes that can be leveraged to enhance cybersecurity in the federal government?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: Integrated situational awareness and in-depth understanding of inherent risks and vulnerabilities require new data visualization, integration and evaluation technologies. Predictive analysis of behaviors is another area that needs far more investment. Expanded modeling and simulation capabilities can be used to better identify vulnerabilities and interdependent relationships, which helps assure the security of critical infrastructures. Information privacy, data loss prevention, and massive analytics are also high priorities for us. We are investigating these and many other technologies through our Northrop Grumman Cybersecurity Research Consortium.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: I see two key areas of emerging technology that should be embraced: malware analysis and predictive analysis. Malware analysis: Many agencies, as well as the private sector, have vast amounts of information about the malware that they are trying to protect against. We need to be able to analyze that information, break it down, and define what the core components are to better associate that to how it effects their environment. Predictive analysis: We must begin to have a much stronger collaborative store of information. We can then begin to use a predictive model to further reduce the risk factor. Once we fingerprint the attack vector, start looking at where they are coming from and the tools the attacker utilizes, we can be more proactive on security rather than just being reactive. Also, reputational awareness of applications allows for a more predictive analysis model.

Are there any robust, successful private-sector approaches to cybersecurity that can be incorporated into the federal space?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: A couple of the large ISPs have built very effective security operations with integrated situational awareness, out-of-band communications across mission management, and a mindset that assumes the bad guy is inside the perimeter. Northrop Grumman has been a recognized leader in this area with our Consolidated Cyber Security Operations Center in Maryland and our holistic, integrated approach to security management. We take a unique, multi-disciplinary approach that includes integrating policies, technology, economics, legal, information sharing, and human factors to address the major threats. The public-private partnerships that are gaining strength and popularity are a great venue for sharing best practices and strengthening everyone's cybersecurity.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: You have seen a lot of the information that has come out; we have talked about the increased amount of malware that is being found today. So this really has created a major increase in the number of signatures – information that is being used that identifies malware and is required to block the malware attacks. There is a large number of attacks in there. This is really not the way to handle this moving forward, because we want to reduce the impact of trying to create more and more scanning that goes on in the system from malware. But we still need to maintain a very strong security model.

How important is universal connectivity among federal cyber ops centers? What would it take to get it done?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

John Bordwine
Public Sector CTO
Symantec

Edward Swallow
Northrop Grumman Information Systems

A: Connectivity is critical among key federal operations centers and becomes even more critical when one or more parts of the government are under active attack. Most connectivity today is "in-band." That means it uses the same network that is being attacked to provide the connectivity. What's needed is an "out-of-band" network that connects the Security Operation's Centers (SOCs) so they can coordinate during an attack and share vital information about attack vectors, countermeasures and information that could lead to the arrest and conviction of the perpetrators. Some agencies have more critical security needs than others, which has led to the current lack of common approaches across the Federal space. Common processes are needed to support effective connectivity and inter-agency collaboration.

John Bordwine
Symantec

A: True situational awareness is being able to define the overall risk and mitigation process of the US government. We must have this universal connectivity between the federal cyber operations centers to be able to have that true situational awareness view and view of readiness we need to take. There has to be a framework that is built specifically for the sharing of information as it relates to threat risk and mitigation within the United States government. That framework has to be molded into place to create that foundation between the various security operations centers. To make that occur without that true framework – to exchange that information and be able to use that information in the best possible format to mitigate risk – will be very difficult.

THE STAND Cybersecurity

Question 9

Industry analysts say that the federal government will be spending $55 billion on cybersecurity between now and 2015, but that the dramatic increase in funding and focus isn't enough to fix the problem. Do you agree with that assessment? Why or why not?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: I don't think it's clear what they will spend on cybersecurity between now and 2015. First, we don't know what the legislative environment will be. Congress is considering major pieces of legislation that could have a huge effect on the money that will be required. Also, there could be a lot of savings if the Federal government could focus on a risk-based strategy for addressing concerns, such as the approach the State Department has taken. Another factor is the potential for a cyber 911, which could drive public opinion to demand stronger, more expensive measures. Factors are still too nebulous for any reliable prediction over the next five years.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: I believe that with any large-scale investment, the government really needs to prioritize cybersecurity efforts. There must be a focus on creating a functional framework – items such as legislation, policy and even enforcement. Policy definition and the enforcement of such must go hand in hand. So without the appropriate prioritization of effort, I think we will see these funds be spent rather quickly and only have limited visible results.

Initiative #1 in the White House's new Comprehensive National Cybersecurity Initiative aims to "manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections." Based on where we are today, what does the federal government need to do to make that happen?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: The Federal Enterprise Network has had thousands of Internet connections. These numbers are dropping to hundreds of Trusted Internet Connections (TICs). It's unclear whether there is sufficient asset management and end-point control to ensure that there are no unknown connections. If each agency is left to manage its TIC in its own way, and to fix vulnerabilities when its budget allows, then the weakest TIC is the hole through which cyber intruders can easily penetrate. Risk management, asset management and end-point management and significant reductions in the number of TICs are all critical. Internally, we manage three TICs for our own corporate network; they're a challenge.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: Managing the US Government as a single enterprise is going to be a major uphill endeavor; there is a lot that has to be accomplished. The [Trusted Internet Connections] TIC itself was developed to consolidate the number of Internet connections, reducing the risk factor to the US government. That's really one basic step to creating a single enterprise network. But collaboration of information is another key step that still seems to be an area of concern. What it teaches us is that there are many aspects, all of which must be enacted to ensure better protection. So the TIC is a major initiative and I think it will reduce the level of risk. But it is only one component and it really does not fully define a single network enterprise.

THE STAND Cybersecurity Question 11

Looking ahead to the next year-18 months, what do you believe will be the biggest challenges for federal agencies and how can you help mitigate those challenges?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: Their biggest challenge will be cyber policy development and implementation. We are optimistic that the new position of White House Cybersecurity Coordinator will have a significant impact in the area. Implementing legislation that affects that policy will also complicate their efforts, but in the long run, may result in significant advances in protecting the government's networks.

We can help mitigate the challenge by demonstrating "what works" and supporting information sharing, collaboration and direct discussions about the key issues with government and industry partners. Information sharing is paramount. As an industry leader in cybersecurity solutions, we have a strategic role in several industry organizations including the Transglobal Secure Collaboration Program (TSCP), Defense Industrial Base, Internet Security Alliance, National Security Telecommunications Advisory Committee, National Infrastructure Advisory Council, and others. Our participation promotes the information sharing that is vital to protecting our enterprise from cybersecurity threats.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: I think there is such an influx of even more data and information, the desire by the attackers to get such information is a challenging factor. If you look at the amount of information we need on a day-to-day basis so that we can make decisions, perform our job responsibilities and enact the agency missions, there is much to protect. The bad guys want to get access to that. So I think that over the next year-to-18 months, protecting this information is going to be one of the highest risk challenges to the federal government.

And there is going to be even more information coming into government agencies of a very proprietary and confidential nature. You still need to make sure you are providing the right level of security for that information. Symantec can help with the biggest challenges, because we really look at that data management model. Simply blocking content as a standard data loss prevention model is no longer good enough. We also know that there are new technologies coming into play – Cloud Computing, virtualization and data center consolidation. These are supposed to help the agency do its job more effectively and more efficiently, but they also mean that we are expanding our data flow outside a normal environment. We have to be able to protect that. So data management is much more than just looking at a single component. I believe that the expansion of data is really going to be the toughest thing to get a handle on.

From a company perspective, where would you like to be in the federal cybersecurity market a year from now? Five years from now?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: Same answer to both. We want to remain the market leader and most trusted provider of services and products that protect our customer's information enterprise and enable their mission in a secure environment.

One area we are focusing on is the need to move our customers to "information protection" from just "network protection." We need to move cybersecurity to a view of "enterprise and mission protection." We also need to move the boundary for "trusted perimeters" closer to where we can control, inspect, and manage that trust easily. In five years, I hope that government and industry have achieved that on a wide basis throughout the U.S. We will never get rid of the threats completely, but we can do much to mitigate them.

A lot of research is underway on protecting data – making it so hard to get data out of the system that you've made the cost to the enemy prohibitive. That's why our cybersecurity research consortium is of such importance. By leveraging the innovative freedoms of academia partnered with industry, we can stay in front of the threat and take the next steps needed to develop game-changing technologies.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: It's tough. You can look at it from a year from now get a good idea; five years from now it's a little bit hazier. What I really would like is for Symantec to be considered to be a technological achievement thought leader that brings in-depth security solutions to its customers. We also would like to be considered to be a major ally to the U.S. Government and its development of its comprehensive cybersecurity model. Even in the next year, that is the goal to shoot for and we are comitted to meeting their expectations. Five years is a long way out. It's a little tougher. I really would like Symantec to be considereda company that has helped drive the convergence of IT management and IT Security Management into a cohesive strategy. It's going to take a little while, but the separation of duties within an organization – and agencies without collaboration – only increases risks if you have not aligned your IT Management strategy and your IT Security strategy. Without this collaboration, you assume more risk. If a well-defined, well-protected system were to be used by someone that inadvertently could be careless, it actually would launch the prevention model. If you don't move to this model, you assume more risk both internally and externally. Defining the right policies can ensure a much more comprehensive approach to IT and IT Security Management.

THE STAND Cybersecurity Question 13

What are three key products/services that you think can help address federal cybersecurity challenges?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

Edward Swallow
Northrop Grumman Information Systems

A: First would be a robust set of services for using Einstein 2 and 3 effectively and then integrating them into an enterprise level management of security. Second would be a product/service offering like the Justice Department's Cyber Security Assessment and Management program (CSAM), developed by Northrop Grumman, which provides continuous Certification and Accreditation (C&A) management to help agencies establish a holistic C&A approach to all systems. Third would be a means for leveraging tools like CSAM and the State Department's iPost across the federal space.

Northrop Grumman's Cybersecurity Research Consortium was formed just for this reason, to help address the cybersecurity challenges of the future. The consortium is taking-on some of the world's leading cyber problems, including attribution in cyberspace, supply chain risk, and security of critical infrastructure networks. The consortium will initially sponsor 10 projects and provide graduate student fellowships, while continuing to expand its portfolio of research to cover the many different aspects of cybersecurity. It is the industry/academia partnership that will leverage the freedoms of academia with the knowledge of federal cybersecurity challenges to generate solutions for the future.

John Bordwine
Public Sector CTO
Symantec

John Bordwine
Symantec

A: I guess it is not going to be a surprise when I say one of them is data management, right? This is not only a product, but also a well-defined policy and a very strong implementation around those policies is very much required. I also think that one of the key elements to being successful here within cybersecurity is being able to have appropriate analytical tools that define the trends and measurable expectations of cybersecurity policies and compliance. Without these tools, you don't know how well you are doing in the way of just meeting your security policy compliance guidelines or your agency definition on what your expectations are in order to meet your mission. You have to have a predictive analysis model. This is really a combination of product tools, process automation and security professional expertise. We really need to move into this model. It will allow us to keep up with the current threat landscape. Symantec is committed to supporting our customers through the changing threat landscape to reduce the risk.

How will the EINSTEIN 2 sensor-based intrusion detection program mitigate the risk to federal information assets? What other assets need to be brought to bear to ensure success?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

John Bordwine
Public Sector CTO
Symantec

Edward Swallow
Northrop Grumman Information Systems

A: Perimeter based defenses don't work very well once the perimeter has been breached. With EINSTEIN 2, we are, in effect "fighting the last war," although its capabilities do go beyond just detecting intrusions. However, we need to get to the next step in protecting data from going out once that perimeter has been breached, or insider threats have been realized. Part of that is a greater focus on data loss prevention as a primary mitigation technique.

History shows again and again that fighting the last war is ineffective. In a webinar that we hosted about protecting critical infrastructures, we posited that there are two kinds of organizations: ones that know they have a bad guy inside the perimeter and ones who don't know they have a bad guy inside the perimeter.There aren't any that don't have a bad guy inside the perimeter. We have seen no serious refutation of that premise, and in fact see much more evidence that we need to get to the next stage, where we protect data as well as perimeters. That will take R&D and serious work, but it must be done, and done quickly. This is where Northrop Grumman Cybersecurity Research Consortium is making inroads. Our company has joined with Carnegie Mellon, MIT, and Purdue to accelerate the pace of taking novel ideas to real-world application.

Another area for investment is better situational awareness, through solutions like the iPost Dashboard for the State Department. Northrop Grumman developed this capability in partnership with its State Department customer. iPost is the technical means to which the Department of State distributed enterprise is continuously monitored for patches/vulnerabilities and attacks. This improved situational awareness needs to be coupled with more effective defense-in-depth approaches and integrated alert and warning processes across the federal infrastructures.

John Bordwine
Symantec

A: Network-based technologies are great for understanding the data that is on the wire and being able to act upon these defined threats that are embedded into that data flow. This does mitigate risk of one variable, but as we look at it, we cannot forget about the other variables such as information protection, data exfiltration, encryption and attack vectors such as email and Internet activities. Also, a part of what still needs to be focused on is end-user education, which is key to reducing risk. So the Einstein 2 Sensor Phase Intrusion Protection Program is a great start at looking at the data in motion and data on the wire, but there are other areas of focus as well.

The goal of the next-generation EINSTEIN 3 approach is "to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response". Are current technologies and processes up to the task? Why or why not?

Edward Swallow
Vice President, Business Development, Civil Systems Division and Lead for Civil Cyber, Northrop Grumman Information Systems

John Bordwine
Public Sector CTO
Symantec

Edward Swallow
Northrop Grumman Information Systems

A: Next-generation cybersecurity approaches will take the next step from protecting the perimeter to looking for bad behavior, adding behavioral analysis to find the bad guys that are inside the perimeter. This is necessary, but still doesn't get to the heart of securing the data itself. Current technologies are up to the task based on known threats, but current processes including governance are not, and effective concepts of operations for new approaches still need a lot of work. We also need to protect against the insider threat, which will require focused research on how to detect, monitor, manage and defeat unauthorized data deletion, malicious data modification, and unauthorized data exfiltration.

John Bordwine
Symantec

A: I find that Einstein 3 is definitely a move in the right direction. The key will be defining the security policies as they relate to situational awareness. Situational awareness means many things to different people and still contains many variables based upon the environment which is being protected. Einstein 3 has a lot of potential, but the overall approach here must be more holistic when it comes to cybersecurity. It's looking at items such as being able to characterize malicious network activity and enhance cybersecurity chronology. Those are very key components we must focus on, but we have to remember that no single technology actually can be a silver bullet to defeating the attacks. On cybersecurity, there must be a holistic approach. Even with Einstein 3, we must bring multiple products together with multiple areas of information so that we can start defining true situational awareness.