Cybersecurity

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

Derek Tumulak

Vice President of Product Management at Vormetric

Cybersecurity has emerged as a top priority for both government and industry. Three cyber experts share their views on the current issues, how threats have changed, and how budget-constrained agencies can defend against Advanced Persistent Threats.

Q1 How do agencies balance the need for compliance with the Federal Information Security Management Act (FISMA) with the demands of meeting evolving security threats?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

To strike a balance, we need FISMA reform to get requirements up to modern standards. Understanding the security "state-of-play" for information systems is essential in today's dynamic environment. We're at a point now where annual compliance checking isn't enough. Continuous monitoring versus just spot-checking once-a-year is critical to preventing adversaries from exploiting vulnerabilities that result from a static environment.

But continuous monitoring is just a start. You need to look beyond your own your own borders – to not only monitor yourself at the edge, but also to think about the threats coming at you. Whether you identify threats by sharing information with peers or by some other means, it makes you more proactive. That's why a continuous monitoring and threat assessment approach is so important. This approach will allow agencies to better evaluate the threat, automate processes to reduce costs, and track the security state of play.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

FISMA initially focused on annual written audits. We are rightfully moving away from that to continuous auditing. That is much better in terms of getting real information in somewhat real-time into a situational awareness tool that actually gives the [cybersecurity expert] information on how he's doing. It allows one to get a level of performance that they have never really had before under the older FISMA requirement. I'm a believer in automating and supporting continuous auditing to a set of standards.

But I think many of us in this business believe it's insufficient. It takes care of maybe 80 percent of the work it helps you lock the doors and the front windows. But for the most sophisticated threat you need to go beyond compliance. You need to dive into intelligence driven defense capabilities developing what Lockheed Martin calls the cyber kill chain. And you need to hire the right talent, very strong [cybersecurity] intelligence analysts who can create processes that go well beyond just a set of compliance criteria.

Derek Tumulak

Vice President of Product Management at Vormetric

I've always felt that any security strategy should take a blueprint approach to addressing compliance requirements as well as actual security threats. That really speaks to best practices. If you take an approach where you are applying security best practices, you are going to address a large percentage of both compliance requirements as well as the evolving security threats that come your way. Meeting compliance doesn't necessarily mean you are secure, especially as the environment changes. Many people mistakenly assume that, because they've checked off the boxes to meet regulations, they're safe. As an example, your data centers evolve, and you've got physical and virtual security, and you've got cloud environments added into the mix. I think it is having this blueprint in place is vital, so that when something new comes around, you are not starting from scratch – you are instead applying, extending or enhancing your existing blueprint.

Q2 Government agencies find themselves dealing with more and more advanced persistent threats. What kind of changes does this require in their cybersecurity posture?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

Installing a couple of anti-virus and malware detection devices on your network won't mitigate the advanced persistent threat (APT). The APT drives you to a more integrated cyber solution. That means I've got to look at defense-in-depth as well as defense-in-breadth. Defense-in-depth means protecting the perimeter, the network, and then again at an end-point or mobile device. Defense-in-breadth means implementing multiple solutions at each layer of defense, from different partners. If it's a solution that's available off-the-shelf, then it's highly likely that the APT also has it, and knows how to get around it. Both for our own defenses and those of our customers, we advocate an architecture called The FAN™, which combines multiple layers of advanced defenses with the flexibility to accommodate changing cyber policies, technologies, and threats without compromising speed.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

With advanced persistent threats, we used to believe that the adversary always had the advantage: The defender had to get it right every time, but the adversary just once. But we believe the aggressor has no inherent advantage today.

That's because we have now dealt with them for a decade and so we are becoming a lot more familiar with them. Yes, they are growing in sophistication, but their persistence is actually their weakness. Because they are persistent, they exhibit behavior and patterns that allow us to anticipate and predict intrusions. We now [recognize] that they have a series of seven steps that they must take in a sequential pattern before they can steal intellectual property or degrade the network -- and we have built capabilities around each one of these seven steps. We call it the Lockheed Martin Cyber Kill Chain™.

If you stop them at all seven steps, they will have to change their entire mode of attacking you. And this is a game of economics: They want to be fast and efficient. They don't want to take a lot of time doing this. So we have really put barriers in the road that make them slower, that make them less efficient and make it more costly for them to execute on their objectives.

This is a big change. We call it intelligence-driven defense.

Derek Tumulak

Vice President of Product Management at Vormetric

Attackers employing APTstyle attacks are just much more knowledgeable now; they are giving priority to a particular set of targets, and they have a clear objective in mind. This really requires government agencies to raise their level of sophistication in protecting against such attacks. Many solutions on the market today have been designed to prevent or at least reduce the likelihood of APT attacks. In addition to preventing or reducing APT attacks, governments can focus on the data itself. Typically, one of the primary objectives of any attack is to get access to sensitive information. Government agencies – especially those that rely on distributed networks – must prioritize the protection of their data through centrally managed encryption, strong key management and strict access policies. Particularly on the access policy side, if you can limit the amount of data that even a privileged user can access, that greatly reduces the impact of these types of attacks. Government security officials must think beyond basic compliance and embrace holistic security best practices protect from data breaches while also ensuring control of the data.

Q3 Cybersecurity experts increasingly talk about the importance of situational awareness. What does this mean in the context of cybersecurity? What goes into developing situational awareness?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

That is probably the question I get the most often from operationally-focused customers who are interested in our cybersecurity solutions: How can I get cyber situational awareness out of this integrated solution that you are providing? They know that situational awareness means one thing on the battlefield, but it means something totally different in cyberspace. In cyberspace, situational awareness means understanding what's going on in your network. Perhaps a device is not performing up to speed because it's under duress – what impact will that have on your overarching mission? Think about it in terms of a large military operations center. It is critical for operators to integrate cyber situational awareness with combat situational awareness. This way, if the network is attacked, commanders will be able to quickly assess how an enemy cyber intrusion will decrease mission effectiveness.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

It's like any other situational awareness that we talk about – from commanders on the battlefield to operators of the network to the quarterback sitting behind the center. Situational awareness means that you are aware of your surrounding environment, aware of the threats that you face in that environment. These requirements exist not only for a quarterback but for those who want to defend their information and their networks.

So, situational awareness involves having some means of getting information in real time that can help you make decisions about how to protect yourself. In part, that means putting sensors on the network, so you can receive status updates on how well you are doing and how well your mission is operating. You want indications or warning sensors that identify barriers to success, be it intruders or network failures.

The commercial world provides many great tools and capabilities that organizations can use to defend the desktop or an entry point to your network. But what we try to do is integrate these specific tools, so that they are communicating with each other. This is part of situational awareness.

Derek Tumulak

Vice President of Product Management at Vormetric

Situational awareness in general deals with environmental variables related to time and space. As an example, think of Y2K. There is the potential for attackers to exploit a weakness in a computer system or a particular organization during a specific timeframe. In cybersecurity, situational awareness relies on security best practices being baked into an agency's daily operations. That means being prepared, as well as having very good real-time security intelligence. There are a number of vendors that provide security intelligence through logging and reports, allowing agencies to make solid decisions in defending against cyber attacks. It is prudent to look at technology solutions that protect sensitive data no matter where it lives, as point solutions by their very nature provide only limited visibility. Once you've got that base infrastructure to work with, then it's about getting data that's relevant to the situation in question. This fundamental approach to data security allows organizations to protect what matters.

Q4 What is being done to spur the development of cybersecurity innovation? What are some of the areas of research that appear to be most promising?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

Cybersecurity innovation comes from numerous sources - universities, government, within companies – even from our high school interns.

Both at the university level and in-house, we're researching cloud, mobile devices, encryption, and identity management – all areas that are promising for innovation. Our Cybersecurity Research Consortium, which includes Carnegie Mellon, MIT, and Purdue, is entering its fourth year providing our researchers new ways to solve complex problems. The Northrop Grumman Cync Incubator at University of Maryland, Baltimore County (UMBC) has been a great way to cultivate small companies and speed innovative solutions to our customers. We also plan to extend the program globally to spur increasing diversity of expertise to combat a threat that has no borders.

Our DoD and Intelligence Community customers are tying efficiency to innovation, and rightfully so. For example, if defenses are architected appropriately, with agility being part of the original design, they can adapt to provide the protections needed for new technologies or services to be introduced. We're also innovating to strengthen the capabilities of our products. The Host-Based Security System we support for DISA is a great example of an evolving capability to handle the wide range and huge number of threats while accommodating emerging platforms.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

We are seeing greater and greater cooperation by companies. We recognized that early on, and so we formed the LM Cyber Security Alliance. We knew that we couldn't possibly expend all of the R&D money necessary to protect every facet of the enterprise, so we have partnered with 18 best-ofbreed technology companies. We take their solutions and integrate them into a seamless fabric that can stretch across anyone's enterprise.

It's this ability to work strategically with our partners understanding the R&D that is coming from them in the future and integrating that into seamless enterprise solutions that separates us from many businesses that have a good idea but can't scale that across a large enterprise. We constantly hear that Lockheed Martin is not innovative – that it's the small business that is innovative. But innovation doesn't come from companies it comes from people. You've got to enable that innovation and use it. A lot of people have good ideas, but if they don't scale across large enterprises they are not very good to implement.

At Lockheed Martin we try to take these great ideas coming from many of these companies and make sure they integrate and scale across a large enterprise.

Derek Tumulak

Vice President of Product Management at Vormetric

We've already talked about APTs. That might seem like it's a little bit in the rearview mirror, but it's not -- there is a lot happening there, a great deal of research is going into how we can prevent these attacks from occurring. There's also a lot of innovation happening in the area of encryption and key management technology. If we really can focus on the data, which could be in a file, in a database, or in an application, and apply the appropriate policies to that data – no matter where it resides – we will take quite a large leap forward in how we protect sensitive information.

We are also seeing significant innovation in security solutions that enable agencies to confidently transition to the cloud while still leveraging many of their traditional infrastructure investments. Lastly, we're seeing quite advanced data security offerings that do not sacrifice application performance or create additional management complexity.

Q5 Many experts continue to worry about the long term development of the cybersecurity workforce in the federal space. What is being done to address these concerns?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

There is much concern over our nation's cybersecurity workforce and whether or not there will be enough trained professionals in the right areas. This past summer, I was privileged to serve alongside a great collection of representatives from academia, government and industry on the Homeland Security Advisory Council Task Force on cyber skills. The group released its final report last October with eleven recommendations for what to do to build a pipeline of individuals with the right skills to be successful in cyber. It's not just one school or one solution; there are numerous ways to build this talent pool - from attending two year universities, to training returning veterans, to standing up a cyber reserve-type force.

The first step is to identify what is really important about cyber and build a competency model around it so you are clear about what you are training people to do. If you just want to have a lot of smart people in cyber, you are missing an opportunity to really define the problem up front. That was our number one task force recommendation.

At Northrop Grumman, grooming tomorrow's cyber workforce is paramount! This year alone, we partnered with the University of Maryland to fund the Advanced Cybersecurity Experience for Students program, which will immerse undergraduate students in all aspects of the field. We funded a grant to UMBC to start the CyberScholars program, which aims to increase the number of women and underrepresented minorities in the field. We are Presenting Sponsor for CyberPatriot, the national high school cyber defense competition, and have developed a Cyber Academy to continue developing our own cyber workforce. Like the threat, our workforce is never static.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

We all compete trying to recruit from the limited talent pool that is out there. You know, Lockheed Martin defends its own global network. It's massive in size, serving 120,000 employees. And because we work on our nation's weapons systems and protect our nation's secrets, we are a high end target for adversaries, not unlike those going after the Department of Defense. So we have a Security Intelligence Center, where we have cyber intel analysts who actually study our adversaries, who study our intrusions backward and forward along the cyber kill chain. But that means finding talented folks. And that means taking six to nine months to train those folks before we put them in an operational environment. But that's too long. It takes too long to give them on-the-job training. So we are trying to speed the process. We have a great need, because not only are we trying to protect Lockheed Martin but we are now selling these [analyst services] to the federal government and commercial organizations. So we have created our own training program, which we call EXCITE™. This program provides high-end, intel-driven defense training programs that reduce the amount of time it takes to get a cyber-intel analyst onto the floor. The bottom line is we are recruiting from within the company, finding people who have cyber skills and taking them to a new level.

Derek Tumulak

Vice President of Product Management at Vormetric

In the last four or five years, I have seen a lot more interest in being able to leverage commercial off-the-shelf (COTS) products and services. What if you could implement a COTS version of smart cards in a secret or top-secret environment? Not starting from scratch is really the notion here. I've talked to several people in government who are trying to take advantage of things like Amazon Web Services or any other leading cloud infrastructure provider. Amazon has that incredible scale, and they don't want to build out that whole infrastructure again. They can use Amazon to get 80 or 90 percent of the way, and then apply the specifics for their government agency. The cloud security vendors have sophisticated enough solutions to provide the required security for data in both public and private clouds. It's really about relying on commercial organizations to get them most of the way there, and freeing up their own workforce and resources to focus on what they really need to worry about. The public and private-sector should continue to collaboratively work on information sharing and risk management, and promote cybersecurity awareness. In the end, it's about providing a high degree of control and sophistication in an elegant manner to protect the sensitive data that matters. For Vormetric, that's data security simplified!

Q6 Many federal officials remain worried about the security ramifications of cloud computing. How much risk comes with cloud computing – and to what extent are those vulnerabilities addressable?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

Addressing security risks in cloud computing is generally a factor of the type of cloud that meets your mission needs. For instance, a private cloud, which is seen as more secure but also more costly than the public cloud, may be right for your mission. Vulnerabilities do exist but they are addressable. It's imperative that both private and public cloud systems be designed with security upfront so customers are comfortable with using it to store their sensitive data and important analytics.

Cloud security is a major investment area at Northrop Grumman. Our Trusted Cloud approach takes defense-in-depth one step further. Since the challenge with cloud security is that the "perimeter" is blurred, classic defense-in-depth will not be sufficient. Cloud requires a new approach to security including protecting the data rather than the perimeter (Information Cloaking) and building "trust relationships" between entities. "Identity is the new Perimeter," and for cloud, Identity needs to be interoperable and portable between clouds. Cloud will also rapidly push the concept of Bring Your Own Device (BYOD) like smart phones and iPads. To handle BYOD requires higher layers of secure mobility including secure "Data in Motion" (from hand held to the data center) and secure "Data at Rest" (if critical data is to be stored in the public cloud).

Our Cybersecurity Research Consortium is also researching cloud security solutions and rolling those new technologies into cloud offerings, so that we can keep the performance and the cost benefits of the cloud but not give up any security.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

Cloud computing is definitely more secure than traditional networking as you have more control over configuration and who and how one can access the cloud. The security controls can be more easily automated, verified and maintained.

People argue that with cloud you're putting all of your eggs in one basket, so if you do have a security breach it becomes more significant. But often, in an enterprise network, you've got system administrators who do cybersecurity as their second duty; their first duty may be something else entirely. Do you want to put your golden nuggets in a cloud where you have cybersecurity professionals providing automated tools and services, or do you want to have a distributed network where many people are in charge of security and they may not be well trained or have updated tools?

When you are talking about cloud security, you are talking about the talent that comes with operating and defending that cloud. You are also talking about the new tools that can do automation of security. You can automate and virtualize your security across the entire cloud and have continuous auditing going on. It is much easier to do in a cloud than it is across a geographically diverse network.

Derek Tumulak

Vice President of Product Management at Vormetric

The most obvious vulnerability with cloud is that your data is no longer completely under your control. If you look back 10 years, your typical data center had all of your data living in your physical infrastructure, on your own servers. Nowadays, with virtualization and the cloud, your data might be under your control logically, but physically it's living out in Amazon Web Services or in some other infrastructure that you don't have control over. That's the biggest security threat that comes into play.

Addressing these issues comes down to applying many of the security practices that organizations might not have felt that they had to in the past. If everything is physically under your control and your employees are the only ones who have access to it, that gives you a high level of assurance. When data is not under your control, you have to take a different approach. You want to apply encryption, strong key management and very smart access policies to the important data that is living in the cloud. That is the only way to gain the level of security control you need.

Q7 Given tight budgets, many agencies are looking to bring-your-own-device policies to jumpstart their mobility initiatives. How can they avoid getting out ahead of their own cybersecurity capabilities?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

I think the key to BYOD is thinking ahead and making the decision that BYOD IS going to be a part of our everyday lives. By making that commitment upfront, agencies can figure out what steps need to be taken to get to a point where they are comfortable with people securely accessing data and mixing their personal life and their business life on a single device that could easily get lost or compromised. If we do that, then it's much easier to plot out the steps to reach that comprehensive endpoint. I think it is going to take a much more strategic look at this issue and coming up with some innovations that will support a strategic plan, rather than a step-by-step approach that starts from where we are today.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

Lockheed Martin is doing a pilot in BYOD. It's about financial and employee efficiency. The financial part is that a company doesn't have to pay for that end-user device. The user pays for it and signs the service agreement, with the business arranging to share some of the cost. It's a good deal for the employee and a great deal for a business. So there is great financial incentive to do it.

There are also operational efficiencies. I don't know about you, but I carry two devices – my own personal device and my Lockheed Martin device. It's a real pain. I really would like to be able to do my personal work and my Lockheed Martin work on the same device. But right now there are technological and cultural barriers to having one device, and they are related.

[One barrier is privacy.] Like any individual, I don't want my company snooping into my private e-mail. And I think Lockheed Martin wants to make sure that my private work doesn't somehow get into my Lockheed Martin work. And then suppose I have a single mobile device and there's an intrusion and the device is compromised. Does the whole device have to be wiped? If so, I would lose all my personal pictures, personal e-mails and everything else. The crux of cybersecurity doesn't change just because the devices get smaller. The concept of containers and virtual machines has been around a long time and computers have been multi-purpose for decades. In short, we have to address the same threats and adversaries, just on more platforms and for broadened user CONOPS now. Those with expertise in cyber are using it to defend the mobile network and those without robust cybersecurity practices are at risk of serious data compromise."

I am glad to say that there are good technological answers. Lockheed Martin will be introducing a secure enterprise mobility product that will allow an individual to do personal work and company work on the same device. It will place a container on a personal device that includes identity protection. A user can go into this environment and do work-related work, and then come out of it and do their personal work. We can separate those two, secure those activities and ensure privacy of both. The product is ready. It's being piloted right now and will be publicly available in the second quarter of next year.

Derek Tumulak

Vice President of Product Management at Vormetric

A lot of this depends on the need to take a BYOD approach. There are vendors that have solutions that address this – mobile device management solutions, mobile data protection – and those are very helpful, making it possible for government agencies to allow various mobile devices to be used. If you implement the right solutions, you should be fine. If not, then the other approach is to strictly limit which mobile devices can be used.

Q8 Encryption is often touted as an important element of cloud and mobile cybersecurity, yet many people worry about the impact on performance. When is encryption a good investment?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

Encryption is always a good investment, because the encryption technologies are widely available and they are not that challenging to implement. But people don't do it because either they don't understand that encryption is a good thing to have, or they think it will have a big impact on performance. But just think about your wireless network at home. If you've got free and open access, your neighbor can access your Wi-Fi. But if you've got at least basic web encryption, or some of the more advanced encryption techniques, I can guarantee that you won't notice any performance difference, yet you've taken a significant step toward limiting access. Encryption overhead is not a big deal in today's environment of fast Wi-Fi and 4G-type networks.

Encryption of data in transit is important, but encryption of the endpoints is also important. People who have laptops or other devices that don't encrypt data at rest are really playing with fire. If somebody steals your device and the hard drive is encrypted, they are probably going to reformat it and start over. If the hard drive is wide open, I can assure you, they are going to poke around.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

The use of encryption for the protection of data, whether at rest or in transit, is critical. As a general rule, all data in transit and any data stored on a mobile device should be encrypted to prevent the data from being stolen. In addition, it is strongly recommended that any data stored in a cloud should also be protected by encryption due to the shared nature of the environment. But from a practical point of view, it is critical that any sensitive data, at a minimum, be protected. Security Policy should be used as the driver for what is required to be protected and at what strength of encryption. As for performance impact, most of today's devices have powerful enough processors so that the use of encryption will not be noticeable to most users.

Derek Tumulak

Vice President of Product Management at Vormetric

Encryption has been around for a very long time, but we are seeing it rapidly become mainstream for two reasons: 1) the amount of data that is being migrated to private and public cloud environments is enormous; and 2) advanced encryption solutions get the job done without being complex to manage. Encryption is a good investment when you have negligible performance impact. There is a high level of transparency, in that you don't necessarily realize it's there, particularly from the end-user's perspective. But you've also got strong key and policy management, so your security team can apply the appropriate levels of control on the data that you need to protect.

Q9 Smart card-based identity management makes it possible to develop an integrated solution for securing facilities, networks and data. What are the advantages of such an approach?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

One of the big advantages of that approach is that it requires you to have something physical to access your network. You don't just need a password to log in. You've got something in your hand that you are required to put into a machine and then type in a PIN or password on top of that. So right away you get the advantages of two-factor authentication. Northrop Grumman went to an entire smart card approach for all of our identity a couple of years ago. We were one of the first in the industry to adhere to the federal standards and deploy a system where employees can securely exchange information with the U.S. government. Every single Northrop Grumman employee can use their badge both for access to our buildings and access to our computers. We talked earlier about advanced persistent threats. Part of their intent is to steal your credentials. If my smart card is one of my credentials, that is a lot harder to duplicate or steal.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

As Richard Hale (the chief information assurance executive at DISA) taught me, when you have a smart-card it requires two things: something physical and something you know. The security increases over a password. [And with converged security,] the cost-efficiencies are fantastic. I have four cards around my neck, which is inefficient.

And because identity [management] is so critical you are seeing a lot of different ways to improve security besides the smart card. It's similar to encryption. You want it to be an enabler but without putting the user through a lot of pain and agony. So that is the key to any identity solution you want to use: It needs to be very simple for the user, and yet foolproof, ensuring that that identity is always associated with only one user. Today, we see alternative approaches to smart cards including "one-time" code and simple approaches such as biometric fingerprints, gesture or voice recognition.

Derek Tumulak

Vice President of Product Management at Vormetric

I previously managed solutions that included smart cards and other multi-factor authentication. The advantage is that it's not just what you know, but in the case of a smart card, it's having something that can physically validate who you are. Of course, there are other factors that can come into play as well. Retinal scans, fingerprinting and many other types of authentication exist in the market today. Smart cards are great as a form of multi-factor authentication; going forward over the next several years, I wouldn't be surprised if we see a lot of innovation happening in this area.

Q10 A recent report found that the most frequent culprit in data breaches is an employee, not a hacker. To what extent can technology address the insider threat, whether it's malicious or simply careless?

Mike Papay

Vice President and Chief Information Security Officer, Northrop Grumman Corporation

Part of this can be addressed through technology, but part of it can only be done through education. You must continuously educate your employees about how to be careful at work. One of the ways we do that at Northrop Grumman is by spear phishing ourselves. We have an internal spear phishing program that my team sets up to send e-mails to a lot of employees, and then we gather statistics on how we do. If you click on the link in one of these messages, it walks you through a process that educates you about what is suspicious in the email and what you should have done.

You can also address pieces of the insider threat through technology. We are piloting some advanced techniques inside our own network that look for what you might call "off-nominal" behavior. If somebody is doing something on an everyday basis, but then one day that person downloads a large amount of information onto a CD or a thumb-drive, that might tip me off that something might be wrong. It's very likely that this person is burning that CD to give to a customer and that it is valid data. But at least the system gives you a "Look over here and pay more attention to these kinds of activities" approach.

Charles Croom

Vice President of Cyber Security Solutions at Lockheed Martin

It certainly sits near the top of the list of hard problems, but it's doable. A lot of the work being done goes back to the fact that every individual is an individual and each of us exhibits our own patterns and behaviors. If you can monitor those patterns and behaviors and look for deviations, you can discover a lot of things. That is an area that is being aggressively pursued.

The second thing is that individuals are still the weakest link. For example, phishing e-mail is still the number one threat to companies, followed by users going to websites that contain malicious code. . At Lockheed Martin, we have a continuous training program called the I-Campaign. Before starting this, the company sent out company phishing e-mails to test each of the users and create a baseline measurement. Then they developed one-minute video games that educate desktop computer users about cybersecurity. They make it educational, but they also make it fun.

Then they started testing company employees again, sending e-mails that would have some obvious indicators that they probably were not good e-mails, such as misspellings and a bad sending address. If I elected to open it anyway, up it comes and says, "Charlie, you didn't do that right. This was a company phishing e-mail and you should have noticed the following..." And if I fail a number of these, my boss gets notified. So what have they done? They have got my attention. Now I am looking at these e-mails coming in and I'm asking, "Is this a test, or is this a real e-mail?"

I Campaign has done quite well for us. We also sell this capability, and some of our more sophisticated users are buying it, because they recognize that the desktop user if trained appropriately, can be a first line of defense.

Derek Tumulak

Vice President of Product Management at Vormetric

Purely on the technology, I think the goal is simplicity – to make the technology as simple as possible. If you don't make it simple, one of two things happen: people make mistakes, because of the complexity, or they decide not to use the technology and work around it, because they don't think it's worth their time or it creates problems for them. One term that has come up in the commercial market is the "consumerization of the enterprise," and I think you could apply the same concept to government agencies. It's just got to be simple. Five or 10 years ago, it was "Send me patch #11 and I'll work with it" – I think the tolerance for that is slowly going away.

Running parallel to this is the notion of social engineering, where you can coerce people or manipulate people to do things. The people are not malicious, but if you lead them down a certain path… The typical example is you leave a bunch of thumb drives in the reception area. Someone picks one up and sticks it in his or her computer. With things like that, it goes beyond technology – it's about education, policies and guidelines. •

theStand