Vormetric on Cybersecurity

Derek Tumulak

Vice President of Product Management at Vormetric

Cyber threats take many forms and come from many directions. But in many cases the target is the same: The data. That is why Derek Tumulak, Vice President of Product Management at Vormetric, says that whatever other measures agencies take, they need to ensure the security of that data. It's also vital to rely as much as possible on proven commercial technology and best practices, rather than building solutions from scratch.

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?

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?

Attackers employing APT-style 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?

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?

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?

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?

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

Vormetric on Cybersecurity

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?

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?

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?

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?

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.•