

Encryption and Database Activity Monitoring – an Interview with Gretchen Hellman – VP Marketing for Vormetric

Listen to the Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Brian Contos: Joining me today is Gretchen Hellman. Gretchen has over 10 years of enterprise security and enterprise software experience. She is the VP of Marketing and Product Management for Vormetric. Gretchen has held product marketing and product management positions at companies such as Voltage Security, ArcSight, and McAfee. She holds a Bachelors of Science in Electrical Engineering from Santa Clara University.

Hi, Gretchen, thanks for joining us today.

Gretchen Hellman: Hi, Brian, it's a pleasure to be here.

Brian Contos: We tend to find ourselves doing a lot of media activity these days, and I was glad when you decided to come on and join this podcast. You have a lot of very interesting perspectives on security, especially data security, so I think this will be an interesting conversation.

Gretchen Hellman: Well thanks Brain, I always love our conversations about security.

Brian Contos: Before we get started -- and you know I do want to dive into data security in just a moment. This is sort of a tangential topic, but I know you have been hounded by the press lately about the Heartland data breach. Maybe you could tell us a little bit about that and some of your perspectives on that.

Gretchen Hellman: Yeah, sure. The Heartland data breach is believed to be the biggest data breach in US history, 100 million plus records stolen from one of the largest payment processors. Now a few things make this interesting. First of all, the fact that the attack was relatively sophisticated. There was malware that launched a sniffer, the sniffer was able to collect cardholder data and send that outside of networks. That's the current belief; that's what the Secret Service believes. They believe that suspect is someone outside of the United States. And then it shut itself off.

So just the increased level of sophistication in data theft for profit is just staggering. There's real money there, and that means that payment processors and anyone with valuable personally identifiable information has really got to step up the security game.

The second piece that's really interesting about this is that Heartland had been responsible, according to the letter of compliance. They had been certified as having been PCI DSS compliant, they got that certification about six months before the breach.

You and I have talked a lot in the past about: does compliance actually provide strong security, or are they mutually inclusive or mutually exclusive? And I think this really will hopefully cause some rethinking in terms of how compliance is performed. Whether it is a universal checklist of items, or whether it incorporates some element of risk, and looking at the individual systems and processes of the organization.

Brian Contos: In the two points that you brought up, the first one, the sophistication of the attack and the fact that much of this is probably spawned from people that have some level of resources. And I don't know if that's organized crime, nation/state threats, terrorist organizations, pick your thing, whatever it is. But it's somebody that has, or some group of people that seem to have, more resources to point at these attacks than the typical hackers of old. And this is something that I think security professionals have been talking about for years, it's been on the top 10 list for as long as I can remember, that attacks are becoming more sophisticated.

But now we're seeing things like this, where it's somewhat sophisticated in approach. We're seeing hardware based attacks. We're actually seeing devices being soldered into systems that are connected to mobile devices and capturing people's credit card information.

And these are very sophisticated attacks. Is this a trend? Should we expect to see an increase in the sophistication of these types of attacks, and possibly the resources that organizations have that are launching these types of attacks?

Gretchen Hellman: Well I definitely would agree with you there. I mean, we are in a constant cyber arms race. So the more difficult the systems are to bypass, the more sophisticated the attack mechanisms will become. And you and I have talked about this a lot, it's a cardinal rule of security: nothing is ever secure. You put as many controls in place to prevent someone breaching it. And the level of controls, or the difficulty of the controls you have to put into place, have to be just more -- or if it doesn't cost you much -- significantly more than the resource somebody would want to put towards getting that information.

So information is now far more valuable. There's a business there, there's a black market for information, so those resources will continue to go into trying to find more sophisticated ways to attack the large repositories of information.

Brian Contos: I think it really amplifies the need. And again, this is something people have been talking about for years, which is defense and depth. And having a solution or groups of solutions, whether it's technologies, policies, or awareness and various approaches; your defense can outrun the offence. Because as you mentioned, it is a cyber arms race. And certainly in the future, I think we're going to see a lot more things that are targeted. And they're going after the crown jewels, they're going after data.

And I think everybody agrees that we're far away from the days of hacking for notoriety. We're actually seeing people doing this -- purely profit driven. Whether it's intellectual property, patient healthcare records, financial data, what have you.

And it's funny, it reminds me of a item I just blogged about earlier this morning: I was talking to a friend of mine about NERC and an auditor that came into an electric company. And essentially the company themselves said, "Hey, while you're doing this, could you do a risk assessment of our cyber security infrastructure?"

Which is what NERC is focused on for the electric industry. And they were actually told by the auditors, "Oh don't worry about the security assessment, we're just here to check to see if you're complaint." And I really think that's...

Gretchen Hellman: Wow!

Brian Contos: To me that sums it up right there. And I've always been a big fan of saying, "One form of compliance, even per industry, it's no blanket." You have to look at the various circumstances, the architectures of what you're trying to protect, how you're doing, et cetera. Everything has to be handcrafted per that organization. But to see this mentality and this logic now coming from an auditor, just makes you wonder how bad things really are out there.

Gretchen Hellman: Yeah. That's a very impactful example. And one of the questions I've been getting asked a lot with the Heartland data breach is, "Is PCI DSS useless? Does it provide anything?" And I'd say: Compliance, like PCI for example, isn't useless per se. I mean, it has driven organizations that maintain cardholder data to put in more controls. But it's all about the philosophy of how you put in those controls.

And then it's about covering the additional bases. So for example, if you just go, "Put in a box," so that your auditor looks at the box and then checks the subsequent box on the compliance list, that's one thing. But if you're spending the money anyway, you might as well really take a look at what that security initiative needs to do for your organization. And then tighten things up there.

Brian Contos: Exactly. Nobody is in business to be compliant. So if you're going to spend the money anyway, you might as well make yourself more secure. And an added benefit is, you might be able to even improve some business processes and things like that. I'm a huge fan of that. If you're going to spend the money, get the most you can out of it, don't just do the check boxes. Well that's kind of a great segue; let's talk a little bit about data security. Obviously you've been working in security for, I guess, well now over a decade. Isn't that right, Gretchen?

Gretchen Hellman: Oh yes, definitely.

Brian Contos: And a big part of that of course, has been your background in encryption. But why is it -- and this is something that I've been seeing for years -- there's this movement from a network-centric thought perspective around security of old, the firewalls, VPNs, IPSs. To now, one that I would say is more data-centric. And people are now starting to talk a lot more about the applications, the databases, the identities of people, and how they're interacting with those applications and databases. It seems like it's really coming down to those core crown jewels. Is that something you're seeing? And why do you think that's happening?

Gretchen Hellman: Oh, definitely. Well I think it's a number of factors. I'm a big fan of Maslow's hierarchy of needs, and basic perimeter security was the food/eat, basic food/eat/shelter. You needed to protect the inside from the outside. And then of course in '03 and '04 we saw a huge push towards systems level security, because malware attacks were starting to get so much more sophisticated. Now we find ourselves in 2008. What we've got is we've got data breach disclosure laws, which are driving a lot of interest, because data breach disclosure laws don't make you do anything in terms of security.

You can do absolutely nothing and be compliant with the data breach disclosure laws which 44 states, District of Columbia, and Puerto Rico have. But if the information is stolen and if

the information is not encrypted and if it contains information on residents, then you have to tell everybody. The impacts of that can absolutely cause havoc to your business and can cost tens of millions of dollars.

In the case of card systems, they can even put you out of business. Perimeter security will never be perfect but there are practices those technologies have gotten more sophisticated. It really is time to look at the value of the data we're trying to protect.

It's no longer just continuity of service. It's, "Wow I've got these designs and these designs are my company's IP. How can I make sure that that's protected at all times and not stolen? How do I maintain my customers' trust? How do I avoid a data breach?"

Brian Contos: You know what that makes me think of? You think about security and a lot of us came up from -- I know myself I came up from the network administration system administration space. Security was thought of in terms of you stick up a firewall. You block some ports. You add some patches. It was all very structured. It was funny. I was listening to a conversation just the other day and they said that network security is a little bit like Lego's. When talking about data security it's a little bit more like clay.

So I think when people say why is data security so far behind in comparison to network security. I think it goes to your statement. We did what we had to do first. We had to put up these barriers. We had to put a lock on the front door. And now we're assuming that, OK, attacks aren't now about IP fragmentation so you can get through a firewall. They're not about smashing the stack for fun and profit.

What it's about these days is it's about how can I pull your data out, extract that information quickly, easily and hopefully not leave a big footprint. And the firewall doesn't care because I'm doing this all over a port that I'm supposed to be going over anyways.

It's the different mindset I think. When I talk to a lot of the folks on the data security side, they came up from it from an application coding perspective or a DBA perspective. So it's a little bit of a different mindset the way that they think about security, network security people talk about it.

I wonder if there's going to be a time where we're going to have folks that converge. It's like we talk about physical and logical. We're talking about data security specialists and network security specialists. What is your perspective you that? Who is making the decisions around data security?

Gretchen Hellman: That's one of the biggest problems is that there really isn't any consistency, Brian. So in a lot of cases database operations are choosing encryption solutions per database. In storage area, the storage guys are choosing it. Without consistency and standardization what this has led to is a total management nightmare. I talked to companies that have over 250 different encryption technologies in their organization and that means 250 different points of key management. And that means that they need an enterprise key manager but the managers just aren't there to support that enterprise management.

The patchwork point solution problem has definitely exploded with the fragmented decision making process. We are seeing the CSO so really strive to work to control that. We're seeing a growth in naming a few standard encryption technologies so you can ensure consistency first of all, make sure that you're encrypting the right things. Then also simplify the management process.

Brian Contos: Is encryption the panacea or is it just a piece of the equation?

Gretchen Hellman: It's definitely a piece of the equation. I would love it if there were one silver bullet for security and personally it would be great if it's technology I was associated with the silver bullet, good for me. Unfortunately that's not the case. You and I have often talked about how there used to be multiple layers of security in an organization. The reason you are encrypting data is because you need to store that data. You need to store that data, because at some point you need to decrypt that data.

So it's very important to take an information management-centric approach when you are looking at your data security program, encrypt when you can. When the data needs to remain whole, you need to provide protective measures in place, such as monitoring and such as prohibiting specific actions that might cause unwarranted destruction, unwarranted thief of that information.

Brian Contos: Yeah, I guess and I have said this before. I'm just such a big fan of the approach of prevention, augmented with detection, augmented with response. Preventative measures are great. They are needed but they are not going to scale. You need to augment it with the ability to monitor and when something does happen and you do need to be able to respond, you do not want this to be an ad hoc situation. You want to have a structured methodology to block.

That could be a number of things. That could be a database firewall, an application firewall. It could be TCP resets, disable user IDs. It doesn't matter, but I tell people what I'm thinking about data encryption, waft, damn, all these things really need to play together to give you that defense in depth.

Gretchen Hellman: Right, prevent what you can. Monitor and audit what you can't. Most definitely.

Brian Contos: Being that we are in the first month of a new year, everyone is coming out with a top 10 list. Everyone is coming out with predictions. What's the Gretchen Hellman prediction for data security for 2009? What are we going to see this year in terms of adoption of new technologies or new attack vectors, vulnerabilities, what's your looking glass tell you?

Gretchen Hellman: Well, I think unfortunately that we're going to see a lot more large in scale, large impact data breaches. Organized crime has figured this out. And we saw it last year with the TJX case. We've seen targeted attacks in the UK on specific financial services firms. We have seen the Heartland data breach now and this is the reality. There's a model now and it works. And it takes time for the enterprise to put those preventative measures in place. So unfortunately I think we'll see some more examples of this. I think that there will be some spirited debate that hopefully ends up in new and improved viewpoints and requirements for compliance and what to really be compliant with the security regulations means.

I think we really are going to see large organizations take a good hard look at their mass of data stores. To really start to get over that hurdle of thinking that they don't need encryption and that they don't need monitoring and prevention technologies.

Brian Contos: Once again I would just like somebody to say, everything is just going to be great. There aren't going to be any attacks. All the vulnerabilities will be gone, but I guess that doesn't happen. I never hear responses quite like that. [laughs]

Gretchen Hellman: Just like military, military warfare has gone from stones and slings to spears to muskets to guns to nuclear weapons and tactical missiles. We've definitely seen the same thing in cyber information protection.

Brian Contos: What kind of parting thoughts can you leave us with today?

Gretchen Hellman: I think the biggest parting thought I can leave organizations with is -- well, maybe I have a couple. You know I'm always bad at boiling them down into one. First of all, a little investment now means a lot of savings later. I was doing a count and something like 8 out of the top Fortune 10 have experienced a massive data breach. That's just raises the whole entire responsibility for every organization.

Second of all, I think the main barrier or inhibitor to organizations adopting encryption is fear. It can be a very scary proposition to scramble up your data. And to trust a program to scramble up your data.

I really have been encouraging organizations to look at advancements, not only for encryption approaches but also to take a hard look at the key management proposition of what they are doing as they move down that path.

Brian Contos: Absolutely, well, Gretchen, as always and I hope we can do this again in the future, it's a pleasure talking with you.

Gretchen Hellman: It's always a pleasure talking with you, Brian. Thanks so much.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

