

## GLBA and the Financial Sector – an Interview with Paul Reymann

Listen to 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](http://Imperva.com), check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at [blog@imperva.com](mailto:blog@imperva.com).

Joining me today is Paul Reymann, CEO of the Reymann Group Inc. Mr. Reymann is one of the nation's leading regulatory experts and coauthor of section 501 of the Gramm-Leach-Bliley Act. Fortune 500 companies have leveraged Mr. Reymann's subject matter expertise to develop successful go to market strategies for information security and technology products and services within key vertical markets.

He has more than 20 years of experience in the financial services industry, including 13 years with The Department of Treasury's Office of Thrift Supervision, or OTS, in Washington, DC.

There, he guided the regulatory agencies technology risk management activities and offered several key regulatory directives and advisories on emerging management issues, including the industry's first regulatory directive on transactional Internet Banking. Welcome to the show, Paul.

Welcome to the show Paul.

**Paul Reymann:** Hi Brian. It's great to be here. Thanks for asking me to join you today.

**Brian Contos:** So Paul, before we begin, can you tell us a little bit about what you've been working on lately.

**Paul Reymann:** Sure, and for those who may not be familiar with The Reymann Group, we've assembled a team of what we call "subject matter experts" from several key industries such as health care and financial services to public sector, energy and retail. What we do is we leverage the years of clinical, and regulatory and operations experience that we have throughout these industries to help our clients to understand how to better enable compliance and business productivity leveraging the right technology solutions.

Our daily client engagements involve working both with the end user communities and technology companies to help bridge that awareness and the streamlined approach, if you will.

**Brian Contos:** Paul, you have a very interesting background when it comes to compliance. Specifically, GLBA. Could you let our listeners know a little bit about what your involvement was with GLBA?

**Paul Reymann:** Sure, happy to and for those that may know the acronym, but may not be sure what it really means, it stands for Gramm-Leach-Bliley Act. They wrote the law or the act if you will, back in the late 90's. At that time, I was a bank regulator under the Department of Treasury's Office of Thrift Supervision. I had been working on some of the first Internet banking regulations that we had to publish, because as many of you may recall back at that time, we started seeing a lot of Internet banking activity.

Banks were creating websites; we had Internet banks charters being formed. So, there was a lot of focus on the use of the Internet and information technology in general, and what that meant is extended risk to the financial industry.

Around that time, Gramm, Leach and Bliley passed the Gramm-Leach-Bliley Act which did a lot more than just data security and privacy. It was focused on financial modernization in general.

The part that I worked on, as one of the banking regulators at the time, I worked on drafting the rules on how banks and credit unions were going to be required now to follow specific practices in implementing information security programs throughout their organizations.

**Brian Contos:** Why was this act really so necessary for them? You mentioned a lot of banks were doing business online. Was there a specific incident that spawned GLBA? Was there some type of event that occurred that really prompted this?

**Paul Reymann:** [laughs] Yeah, actually, and I laugh. You're going to laugh too when you hear what prompted it. This is public knowledge, it was in the press. So, I'm not embarrassing anybody, although I won't name any names. There was actually an elected official, a Congressman, who had gone into a video store and you can imagine what kind of video store it was that prompted a new law. He was getting a video and his personal information was collected at that store about the type of video that he got. It's not the kind you would give your son or daughter. It's not G-rated.

That made it into the press. Everybody found out that this elected official was watching these types of videos. It made an outrage, obviously for a number of reasons. So, when the Gramm-Leach-Bliley Act was passed, again folks who know financial modernization, the issue of privacy were very hot at the time. That single event, I think, was one of the key catalysts that really drove information privacy and data security into the act.

The financial industry is where it started. Obviously, as part of financial modernization. But, as we've seen it's really grown well beyond that. But, to me that was the catalyst. That single event with that one official.

At the time, there were a lot of good things going on within the financial services industry in terms of good data security practices and controls. But, there were no legal mandates to have to do it. They were doing it out of recognizing a need to have to do it.

**Brian Contos:** I see. We're seeing a lot of that today on the critical infrastructure side as well. There's a lot of organizations that are being very proactive, but it hasn't been until relatively recently until many arenas, Power Energy with NERC for one, where there's actually some type of regulation and penalties for not being secure. So, very interesting birth of GLBA. Looking at GLBA today and other things like PCI, which are very prescriptive, or SOX which is very results focused. Do you see a lot of overlap now between some of the groundwork that GLBA laid in things like PCI, and SOXs and others?

**Paul Reymann:** Absolutely, and I refer to this frequently, Brian, when I'm talking as the common threads of security compliance. Just to be clear, GLBA while it's a mandate, it didn't really assign anything new. It just took what we saw happening throughout several industries among high performing leading organizations in the way of their existing best practices that they were doing already, as I mentioned, because of the need to do it.

We took a look at that and said, "Let's get everybody on the same level playing field". Raise the bar, if you will. And we took those best practices and just moved them from optional to mandated, and that's what GLBA reflects is really recognized industry best practices.

If you hold onto that thought for a minute, and you think, "Well, gosh. We have so many legal, and regulatory, and national and international standards out there today focused on technology risk management and information security. PCI, SOXs you've mentioned, and there are many others.

All of these really do stem from the same foundation of traditional best practices.

So that creates a very understandable common thread throughout all of these because they reflect what the professionals have been doing, the people in the trenches who really know the risk and the threats and have been focused on what are the right controls throughout a given industry, whether it's retail, publicly traded companies, healthcare for HIPAA, as we're talking about GLBA for financial companies.

**Brian Contos:** Yeah, that raises an interesting point. I work with a number of organizations that are multi-regulated and those organizations, instead of trying to address HIPAA and then SOXs and then PCI and these various requirements, European requirements like EU, they're actually looking at very low level controls like NIST, NIST 800-53 for example, and then high level ISO controls like 27001. They're even calling it ISO over NIST, and they'll implement practices and procedures and technical controls to address the business requirements at the ISO level, and the fundamental control perspectives from NIST 800-53.

By doing that, for their sort of general risk practice, they're basically addressing all the various forms of regulations and mandates and what have you.

I think that's very interesting now how people are taking a step back, looking at the broader picture saying, "Let's go ahead and build a strong security posture, and in doing so, quite frankly we're probably going to go ahead and address or exceed what some of these things are asking for."

**Paul Reymann:** Absolutely, and I couldn't agree more that the types of resources you mentioned - NIST and the ISO standards are very important because in many cases, they're more specific than some of the other criteria that are out there, so it's a natural migration. People really want to know the tactical detail, step-by-step, how-to type instructions. But what I want to share with you actually, and this is really fresh because we just had a lunch meeting with the folks at NIST about two weeks ago up in Gaithersburg.

We were talking about a lot of different topics and the one at the tail end of the conversation I brought up was, "There's so much overlap and you guys are in such a vocal position right now to issue good standards and guidance. What are you doing to address this overlap and to help drive the awareness of these common threads?"

And they all kind of smiled, tongue in cheek and said, "You know, Paul, we couldn't agree more, and actually we're taking steps now to address it with the ISO standards. We're

## GLBA and the Financial Sector with Paul Reymann

looking to create an alignment or a mapping, if you will, of how the NIST criteria-and you already referenced 800-53, that's a great example.

How that maps control to control with the ISO 27001. And then the goal would be hopefully to do that in reverse as well from the folks on the ISO committee.

For those who may have seen the latest draft that just came out yesterday from NIST on the almost final version of the update to 800-53, they even say that in the first three pages: "Oh by the way, we're looking at the ISO standards and we're going to create this mapping resource." So I think it's very exciting and very important that that gets done and I'm glad to see they're taking the pen on that.

**Brian Contos:** Yeah, absolutely. What a great maturing process for NIST and ISO. I've actually seen a number of people that have done this on their own via extremely large Excel spreadsheets and very complicated Pivot tables and things like that to try to do the mapping. But I think it's the right place to have NIST actually take the reins and do that. That's something I think the industry will benefit from greatly.

**Paul Reymann:** That'll be the right price!

**Brian Contos:** Zero is the right price. [laughter]

**Paul Reymann:** It'll be free!

**Brian Contos:** That's great. When you look at GBLA today...I'll even say this, when you just look at regulatory compliance and other types of mandates like this, what are you seeing as some of the common technical challenges or political issues? And further, what's working and what simply isn't? You're down there in the trenches, you're seeing a lot of this, you're working with high level executives as well as engineers across the board. What's working? What's not working? What are some of the big issues out there?

**Paul Reymann:** Well, that's a great question, and you're right, we have worked with many companies of different shapes and sizes and types over the years to help address these exact types of concerns. Let me just kind of think back to the days when we were putting the final pen to the Gramm-Leach-Bliley Act data security rules, the original version of those because they'd been updated many times through supplemental guidance by the banking regulators.

But at that time, we were starting to see that there was a need for controls to be implemented by not only financial institutions, but others, but we could only focus on the banks and credit unions. And we knew that there was a strong need for certain technology to be there to help make sure those controls work.

I'll give you an example. How do you know that authorized users really only accessed the data they were supposed to and really only used it on a need-to-know basis for the intended purposes they were authorized to have it? At that time, that was highly dependent on policies and procedures-written policies and procedures.

So you're issuing a regulation, you're telling the industry you have to address this, but you know in the back of your mind, that's a black hole, because the technology, while it may have existed, was not cost effective or maybe was not appropriate to fit into the infrastructure of the existing financial institutions.

## GLBA and the Financial Sector with Paul Reymann

But that changed rapidly and soon after that, we started working with a number of companies, Reymann group, bank regulators. Although we've had many conversations with private and public sector on these issues, to clearly articulate more effectively, how does specific technology help with a specific compliance mandate?

Today if you go to an exhibiting event of that at a conference, you might see two types of vendors that talk about compliance. The one I'll call "strategic partner" and the other I'll call "vendor".

The strategic partner says, "Here's how we help you: we help you with specific compliance aspects of the following criteria, and here's how we do it. And by the way, we don't do all these other items. We only carry items three, four, and five; we don't do one, two, and the rest."

That's a strategic adviser, because they know they can't do it all, but they know very well what they can do and they can explain it to you in plain business terms.

The other is a vendor, who just says, "We deliver compliance, we guarantee compliance." There's so much wrong with that phrase. First of all, it's not possible. Second of all, if you step back and ask them, "Great, explain to me how you do that," they're probably going to be a little bit tongue-tied.

So what we see the biggest need for are more comprehensive solutions that can enable real-time proactive continuous capabilities, but more importantly, a clear articulation of how each company addresses the various aspects of security, whether it is reporting, or logging, or monitoring, or what have you, firewalls, unified threat management, IDS's, ITS's.

Be specific how that technology maps to the specific controls that are required, because in the end it is about good security, not about good compliance. We all want compliance, but I would much rather have a company that is secure than one that is compliant.

We have seen has happened there lately, just in the retail industry. They checked the compliance box, but that was at a point in time and the security wasn't there throughout the year, and they got breached. I hope that addresses your question.

**Brian Contos:** Well certainly no one is in business to be compliant. It is almost thought of as what is the easiest and cheapest way we can address it. At least that was, I think, a lot of the early thoughts. You mentioned the retail industry for example, it was always the Holy Grail that we said - Well look if you have to make the investment anyway, we might as well see how we can leverage this to truly improve security, improve operational efficiencies and effectiveness, streamline the business process, and allow you to make more informed decisions.

I think we are actually starting to get there. We are actually starting to see people say - Look, I had to go through this process, but in doing so we have actually done some things that have actually improved our general business process, which I think is really a great win.

**Paul Reymann:** We call that the risk management continuum and you are absolutely right. More and more companies are moving forward in a good way down that continuum.

**Brian Contos:** Certainly kudos to the maturity of the industry. So, a million dollar question, in your opinion, has GLBA helped?

**Paul Reymann:** Short answer, yes, and on so many fronts. We are seeing so much wonderful progress. Not only within the financial services industry but as we have been talking, the rippling wave effect throughout other industries. As I have said, I am not talking about compliance here, I am talking about security. Security of your network, your infrastructure, your information, your patient records in healthcare.

Compliance is important, but it is really just, I mentioned the risk management continuum, compliance is really just a stress impetus that gets you started down that continuum, and it is a key step in helping to start better security practices. So to me, strong security is the goal, the goal for all companies, whether it is for protecting the company, the customers, or the economy at large.

So, I think GLBA has helped a lot. I think it was also the first to really drive this issue to the boardroom, which has been a significant influence. It used to be the back office, down in the basement, behind the glass doors, kind of issue, in the data center. Now it is discussed in most boardroom discussions, because it is a top line for what they are being held accountable for.

**Brian Contos:** Yes, I agree with it. You are absolutely right, there. Security used to be that red binder, covered with the dust, sitting on top of the microwave, in the break room. Now it is definitely something that is top of mind for many, many people. Like it or not compliance is certainly one of the things that helped drive that conversation. So, what is the future for GLBA? Is it maturing? Has it gone all the way it is...? Should we look for different iterations? Has it done everything it is going to do now?

**Paul Reymann:** Yes, that is a good question, and I get asked it a lot in a lot of different ways. One way I get asked they say - Paul, when is all this compliance stuff going to quite down or go away, right? So, I like to say - Guess what? Not in our lifetime. So to me, the future of GLBA is really what I see as the future of security and compliance, on that topic at large. It is really the future as a way of life for us. Whether it is the businesses, or whether it is in how we are handling the use of our home laptops and computers, as well.

Specific to GLBA, we are going to see some continuing updates to that regulation. We have seen the bank regulators issue many updates over the last several years through supplemental guidelines. They do that on an as needed basis to address changing risks to the industry, or changing threats that they are getting a better understanding of. So it is a constant process of monitoring and adjusting that compliance security landscape, if you will.

One of the things I used to love to hear when I would talk to bankers early on, after GLBA went into effect, in year two or three, they would say - Oh no, we are good. We got GLBA covered, Paul. I would say - Oh, well how are you doing that?

Oh we did our audit two years ago and we had our exam, so we checked that box. They just don't realize that it is beyond that. That the threat environment is changing in real-time. It is not even periodic anymore. It is real-time and it is faster than we can take action to protect against it.

I think what we really need to be looking at is not only in terms of GLBA, but where we need to be going as a cultural approach to better security is the need for a more streamlined security process throughout all the organizations.

We talked, Brian, about the common compliance threads, there are so many recipes, if you will, out there that are similar on how to do good security and compliance. There are still

## GLBA and the Financial Sector with Paul Reymann

some differences among them, and I think that creates a little bit of confusion and perhaps hesitancy among some of the players. So I have been pretty vocal.

As you and I have been talking, it sounds like you are as well, about the need to create more common aspects and unified understanding of what all the best practices should be.

I think if we could do that, as NIST is taking a lead to do from a regulatory framework perspective or from a government agency perspective, it is really going to help broaden the awareness and the application of these principals for all companies.

I think that is the future. I think while we will continue to see separate guidelines out there and updates to things like GLBA and other criteria, I think the closer we get to this clearer, unified security approach to cross industries, the better it is going to be for everybody.

**Brian Contos:** It comes to efficiency, as in terms of the technology being leveraged in the processes and in the standards, and people learning from their peers that it really just makes a lot of sense. Well Paul, this has been a fascinating conversation. I think this is a little bit of a departure from what we generally talk about on this Podcast but very valuable, very insightful information. I really appreciate you coming on our program today.

**Paul Reymann:** It has been an honor, Brian. Thanks for asking me.

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



North America Headquarters  
3400 Bridge Parkway  
Suite 101  
Redwood Shores, CA 94065  
Tel: +1-650-345-9000  
Fax: +1-650-345-9004

International Headquarters  
125 Menachem Begin Street  
Tel Aviv 67010  
Israel  
Tel: +972-3-684-0100  
Fax: +972-3-684-0200