

Cyber Crime: What You Need to Know

By Sean Croston & David Baxter

April 2010

The following podcast is brought to you by J.P. Morgan.

David: Hi, this is David Baxter. I'm a Vice President in J.P. Morgan Treasury Services. I'm a product manager for information and transaction security. Today I'm talking with Sean Croston, Senior Product Manager in Treasury Services. Today we'll be focusing on the heightened cyber threat, and what it means for cash managers and for banks.

Sean, do you want to tell us a little bit about your background?

Sean: Thanks, Dave. I manage a team within Treasury Services that focuses on application security, operational risk, and infrastructure services.

David: Thanks for taking the time to join us today, Sean. What do you see as the biggest security challenge facing the banks and cash managers in the environment today?

Sean: I think there's internal and external challenges that we face. Externally, I think our biggest challenge is the increase in cyber attacks and cyber threats. Some people refer to them as cyber criminals or fraudsters, but they're basically organized crime units that operate around the world. That their job is to essentially steal money from banks and corporations. We've read a lot about this. I think most of us have in the last two years or so. Huge, huge potential as far as making money from a criminal standpoint. It's something that is very, very serious in the marketplace right now.

David: We're no longer looking at a lone hacker bringing the system to its knees.

Sean: I'm certainly not saying that can't happen, but that sort of stereotype is not necessarily accurate right now in the marketplace. These are cyber criminals who are very well organized and highly efficient, and specifically are attacking financial market brands and their customers.

David: Can you give us a specific example of their organized structure?

Sean: Certainly. Say five or six years ago there would be perpetrators of crime that essentially try to do many things all at once. Right now the marketplace has become much more efficient. So there are the criminal units that focus on building software, basically what we've all, I think, heard of is malware crimeware. We've also seen very specific groups that can use the software, or their stealing information off of social networking sites and other places on the Internet. We've seen groups who've become very highly specialized in running infrastructure, hosting infrastructure, both legally and illegally hosting infrastructure to launch attacks. And then there are actually the attackers; the folks that are using this information and these credentials to pose as a customer or a bank employee in order to perpetrate a crime.

David: And how do these groups all fit together in this? Do they work together? Do they work independently? What's their structure?

Sean: Well, I think that each one of those groups has become, again, very highly specialized and constantly improving in their own areas. And they coordinate and work with each other. We've seen globally black marketplaces that have come up where people are selling their software on the black market. They're selling information on the black

market. There are groups that historically you would not think worked together from an organized crime standpoint, are now working very well together. It's a much, much more efficient marketplace than it was say even three and one-half, four year ago.

David: These fraud organizations are really able to leverage a base of extremely well trained and sophisticated developers. This seems to be the challenge that we face nowadays.

Sean: Well, I'd say that's true. I'd say they're very smart. They're brazen, operate globally, and often in jurisdictions that are hard to prosecute in. So I would say that's true.

David: That brings up the question, what can we do? There's a lot of press about cyber fraud. Do we need to stop using online banking applications completely?

Sean: No, I don't think that's the case. Although it is a major threat, and it's one that is here to stay, I don't think that stopping use of online banking is the right answer. I think from a bank standpoint and a customer's standpoint, we both have to recognize that this is a common threat to both of us. We are partners based on a commercial relationship, and we need to make sure that both organizations understand that they have obligations in order to protect each other from successful attacks. I think some of the areas that we can do that are in awareness. Again, the banks reaching out to their customers, and customers reaching out to their banking partners. I think what we need to do is promote best practices. What are the things that they do internally to make sure that simple things, like making sure that anti-virus software is up to date and installed; that the patches for browsers and servers are up to date. Making sure that our customers understand that online banking credentials are very important. They need to be maintained, and they need to be tracked accordingly. On the bank side, we certainly understand that cyber threats are not something that are going to go away. They're increasing in sophistication, and we're continually improving our defenses as well as our offensive resources to combat these criminals. So I'd say awareness, promoting best practices, and again, making sure that we're constantly improving the mechanisms that we use in order to ensure a safe, reliable, online banking experience.

David: Anything else about security in general?

Sean: I think that I've talked a lot about more on the technical side, but there's certainly other elements involved. We've actually seen this happen in the marketplace. Make sure that dual control or dual authority in relation to performing a function with an online application is very important. This goes back to earlier I mentioned there are certainly threats both internal and external. Internally, when our customers use our applications we like to see someone, for instance, create a wire and somebody else approve a wire. That's a very good internal control, but we also see it being a very good external control as well. It's not necessarily a very technical solution as much as it's a process solution. There's a combination of good solid technology, but with good solid risk controls and process controls within our corporate community is very important.

David: In other words, both banks and our customers have an obligation when it comes to security, and we both need to ensure that we're taking certain steps in order to maintain awareness within our operations and to ensure that best practices are used to prevent cyber fraud.

Sean: Exactly. It's a partnership between the banks and their customers, both in the use of the right technologies, best practices, awareness, and then making sure that we have the proper controls within both organizations. I do want to add that we've seen our corporate community respond very well in the last couple of years to these attacks. Their sophistication and understanding has grown tremendously. They've come to J.P. Morgan for our perspective on what's happening in the marketplace, and they've been forthcoming in sharing how they see the threats. We've also seen probably I'd say maybe five years ago, security technology being seen as an inhibitor to doing business. That's transitioned into security technologies and processes being extremely important when accessing a proper bank partner.

David: That makes a lot of sense. That really ties together the earlier points you were making about awareness and the relationship between banks and customers and the partnership that is needed in order to be diligent about security in the current environment. And to make sure that we're constantly maintaining best practices. Thanks for taking the time to speak with me today, Sean, and this concludes our podcast.

Sean: Thanks very much for having me, Dave.

J.P. Morgan is pleased to have brought you the proceeding podcast. For more information on J.P. Morgan Treasury services and products visit our website at www.jpmorgan.com/ts.