Interview Keith Gross with Expansion, 28 March 2018

http://www.expansion.com/empresas/banca/2018/03/28/5abaa576e5fdea7e078b45b5.html

TRANSLATION VIA GOOGLE:

BANKING --- Of the European Banking Federation

"Las 'fintech' deberían ver como una prioridad la ciberseguridad"

ENTREVISTA KEITH GROSS Responsable del grupo de trabajo de ciberseguridad de la Federación Bancaria Europea / Gross explica que la banca se toma cada vez más en serio los ciberataques y alerta sobre el bitcoin.

A. Ros. Madrid

Keith Gross (Dublín, 1972) es el jefe del grupo de trabajo de ciberseguridad de la Federación Bancaria Europea (EBF), de la que forma parte la Asociación Española de Banca (AEB), así como el resto de patronales bancarias del viejo continente. Gross asistió a la rueda de prensa en Madrid en la que el ministro del Interior anunció, junto a responsables de la Policía y de la Europol, la desarticulación de una banda de ciberdelincuentes que extrajo más de 1.000 millones de dólares de bancos desde el año 2013.

Gross explica que aún queda trabajo por hacer en este campo, por ello ha pedido que el sector financiero europeo destina cada vez más recursos a combatir estos ataques, hasta el punto de convertir la ciberseguridad en una de sus máximas prioridades.

– ¿En qué consistió su colaboración con la Policía en esta última operación contra los ciberataques?

La Europol nos pidió diversa información, que nosotros aportamos después de hablar con los miembros de nuestra federación. No tuvimos coordinación con los bancos rusos, donde surgió el ataque, pero sí con algunos bancos que prestan servicios en países que forman parte de la federación, como Hungría.

– ¿Es la ciberseguridad una prioridad para los bancos europeos?

Cualquier aspecto de seguridad es una preocupación para los bancos, que obviamente quieren ofrecer la máxima protección a los clientes. Los bancos ahora son más digitales y vigilan la seguridad en estas nuevas áreas. Una de las partes importantes de nuestro grupo de trabajo es aprender de la información que comparten las entidades en toda Europa. Así podemos saber qué ocurre en este campo en Holanda, en Reino Unido o en Alemania.

– ¿Les cuesta a los bancos informar de los ataques que sufren por temor a un daño reputacional?

El riesgo reputacional siempre preocupa a los bancos, pero creo que eso está mejorando porque los bancos entienden que necesitan compartir esta información y que afrontan un problema común al que debe plantar cara. Si, por ejemplo, yo viera a un ladrón entrar en una oficina bancaria, ¿no llamaría a la policía para contarlo? Creo que los bancos entienden más que deben reportar estos problemas. Esta información está fluyendo más en los grupos de trabajo contra los ciberataques y creo que seguirá mejorando, porque es una amenaza a la que se enfrentan todos los bancos. Hoy es uno, pero mañana será otro.

– ¿Ha aumentado el número de ciberataques a los bancos europeos?

El BCE pide a los bancos que supervisa que envíen la información de los ataques que sufren y creo que es algo importante para entender la magnitud de la amenaza. Los bancos sufren ataques a diario y trabajan en la seguridad de sus operaciones, en la banca móvil, en sus aplicaciones y en muchos otros aspectos. Nadie está a salvo de los ciberataques.

– Tras el escándalo de Facebook de las últimas semanas, ¿puede estar tranquilo un cliente bancario con el uso de sus datos que hace su entidad?

Si. La información de los clientes que tienen los bancos se somete a controles muy estrictos. Hay un gran control para asegurarse de que estos datos están absolutamente protegidos.

– Una de las propuestas de los reguladores europeos es que las entidades se sometan a un test de estrés sobre ciberseguridad cada año. ¿Le parece una buena idea?

Es una de las opciones que contemplan los reguladores y creo que es algo muy bienvenido por parte de los bancos. Ya hay comunicación de los responsables de ciberseguridad de los bancos con el BCE, porque quiere saber cómo trabajan los bancos contra los ciberataques y que están haciendo en esta área. Es muy bienvenido, pero creo que es una cuestión de más diálogo, en vez de más regulación. Los bancos tienen ya mucha regulación en distintas áreas y en este campo creo que es muy importante la comunicación para entender mejor estos riesgos. Por ejemplo, creo que es positivo que el BCE recopile la información de los ciberataques y la comparta cada cierto tiempo.

– ¿Hay más riesgos relativos a la ciberseguridad en las 'fintech' que en los bancos?

Hay mucha colaboración entre los bancos y las *fintech*. Son un reto. Estamos en un mercado abierto y la directiva de pagos PSD2 se ha creado para promover una mayor apertura del mercado, pero creo que las *fintech* necesitan vigilar la ciberseguridad como una prioridad, y no diría que lo es a día de hoy. No sé tan seguras como los bancos, porque no están reguladas y trabajan con nuevas tecnologías en desarrollo. Los bancos tradicionales estudian mucho las distintas plataformas en las que entran antes de tomar la decisión, analizando su seguridad antes de decantarse por alguna de ellas y si es demasiado pronto o no para entrar. Las *fintech* deberían evaluar estos riesgos también. Si eres un banco pequeño y tienes una app con 20.000 clientes o eres un gran banco con medio millón de clientes, para el BCE, en ambos casos debes cumplir exactamente los mismos criterios de seguridad. La seguridad para los usuarios debería ser la misma en todas las plataformas.

– ¿Es habitual que los ciberdelincuentes blanqueen el dinero sustraído a través de criptomonedas como el bitcoin? ¿Qué deberían hacer los reguladores al respecto?

Si, los miembros de las redes de ciberataques acuden a las criptomonedas con frecuencia, porque es más opaco. No estoy seguro de cómo debería regularse, hemos escuchado distintos discursos de distintas instituciones en Europa sobre la posible regulación de las criptomonedas. Es claro que estas divisas atraen a los delincuentes porque no están reguladas.

– ¿Se puede cuantificar el impacto en la economía europea de los ciberataques?

No tengo una cifra concreta, pero algunas empresas manejan cifras preocupantes sobre este impacto. No es fácil de medir y es pronto para cuantificarlo exactamente.

Especialista en ciberseguridad bancaria

Keith Gross es el máximo responsable del área de ciberseguridad de la patronal bancaria y de los sistemas de pago en Irlanda, (Banking and Payments Federation of Ireland), donde trabaja desde hace 14 años. Además, lleva siete años siendo el jefe del grupo de trabajo de ciberseguridad de la Federación Bancaria Europea (EBF). También forma parte de un grupo asesor para la Europol en la lucha contra la ciberdelincuencia. Vive a caballo entre Dublín, donde tiene su sede la patronal bancaria irlandesa, y Bruselas, donde se asienta la Federación Bancaria Europea, en cuyos grupos de trabajo participan representantes de los principales bancos del continente.

Keith Gross.

"La información de los clientes que poseen los bancos se somete a controles muy estrictos y están protegidos"

"Los miembros de las redes de ciberataques acuden a las criptomonedas por su opacidad"

"El daño a la reputación preocupa a los bancos, pero han aprendido que deben informar de los ataques"

"Las 'fintech' deberían ver como una prioridad la ciberseguridad"

ENTREVISTA KEITH GROSS Responsable del grupo de trabajo de ciberseguridad de la Federación Bancaria Europea / Gross explica que la banca se toma cada vez más en serio los ciberataques y alerta sobre el bitcoin.

Keith Gross explains that banks are taking cyber attacks more and more seriously and warning about bitcoin.

Keith Gross (Dublin, 1972) is in charge of the cybersecurity working group of the European Banking Federation (EBF), of which the Spanish Banking Association (AEB) is a member, as well as the rest of the banking bosses of the old continent. Gross attended the press conference in Madrid in which the Minister of the Interior announced, together with officials of the Police and Europol, the dismantling of a gang of cybercriminals that extracted more than 1,000 million dollars from banks since 2013. Gross explains that there is still work to be done in this field, but points out that the European financial sector is increasingly allocating resources to combat these attacks, to the point of making cybersecurity one of its highest priorities.

What was your collaboration with the Police in this last operation against cyber attacks?

Europol asked us for different information, which we contributed after speaking with the members of our federation. We did not have coordination with the Russian banks, where the attack arose, but with some banks that provide services in countries that are part of the federation, such as Hungary.

Is cybersecurity a priority for European banks?

Any aspect of security is a concern for banks, which obviously want to offer maximum protection to customers. Banks are now more digital and monitor security in these new areas. One of the important parts of our working group is to learn from the information that entities share across Europe. So we can know what happens in this field in the Netherlands, in the United Kingdom or in Germany.

Do banks find it hard to report the attacks they suffer from fear of reputational damage?

Reputational risk always worries banks, but I think that is improving because banks understand that they need to share this information and that they face a common problem that they must face. If, for example, I saw a thief enter a bank office, would not I call the police to tell it? I think banks understand more than they should report these problems. This information is flowing more in the working groups against cyber attacks and I think it will continue to improve, because it is a threat that all banks face. Today is one, but tomorrow will be another.

Has the number of cyber attacks increased to European banks?

The ECB asks the banks it supervises to send information about the attacks they suffer and I think it is important to understand the magnitude of the threat. Banks suffer attacks on a daily basis and work in the security of their operations, in mobile banking, in their applications and in many other aspects. No one is safe from cyberattacks.

After the scandal of Facebook in recent weeks, can a banking client be calm with the use of his data that makes his entity?

Yes, the information of the clients that the banks have is subject to very strict controls. There is great control to make sure that these data are absolutely protected.

One of the proposals of the European regulators is that the entities submit themselves to a stress test on cybersecurity every year. Do you think it's a good idea?

It is one of the options contemplated by regulators and I think it is something very welcome by banks. There is already communication from the cybersecurity managers of the banks with the ECB, because they want to know how banks work against cyber attacks and what they are doing in this area. It's very welcome, but I think it's a matter of more dialogue, rather than more regulation. Banks already have a lot of regulation in different areas and in this field I think communication is very important to better understand these risks. For example, I think it is positive that the ECB collects information from cyber attacks and shares it every so often.

Are there more risks related to cybersecurity in fintech than in banks?

There is a lot of collaboration between the banks and the fintechs. They are a challenge. We are in an open market and the PSD2 payment directive has been created to promote greater market openness, but I think fintech need to monitor cybersecurity as a priority, and I would not say it is today. They are not as safe as banks, because they are not regulated and work with new technologies in development. The traditional banks study a lot the different platforms they enter before making the decision, analyzing their security before deciding on any of them and if it is too early or not to enter. The fintechs should evaluate these risks as well. If you are a small bank and you have an app with 20,000 customers or if you are a large bank with half a million customers, for the ECB, in both cases they must meet exactly the same security criteria. Security for users should be the same on all platforms.

Is it common for cybercriminals to whiten stolen money through cryptocurrencies like bitcoin? What should regulators do about it?

Yes, the members of the cyber attacks networks go to cryptocurrencies frequently, because it is more opaque. I am not sure how it should be regulated, we have heard different speeches from different institutions in Europe about the possible regulation of cryptocurrencies. It is clear that these currencies attract criminals because they are not regulated.

Can we quantify the impact on the European economy of cyber attacks?

I do not have a specific figure, but some companies handle worrying data about this impact. It is not easy to measure and it is too early to quantify it exactly.

BOX: Bank cybersecurity specialist

Keith Gross is the head of the area of cybersecurity of the banking employers and payment systems in Ireland, (Banking and Payments Federation of Ireland), where he has been working for 14 years. In addition, he has been the head of the cybersecurity working group of the European Banking Federation (EBF) for seven years. He is also part of an advisory group for Europol in the fight against cybercrime. He lives on horseback between Dublin, where the Irish bank employers' organization is based, and Brussels, where the European Banking Federation is based, in whose working groups representatives of the main banks of the continent participate.