Os Cibercriminosos são os Ladrões de Bancos da Era Digital

Cybercriminals are the Bank Robbers of the Digital Age

Wim Mijs

CEO da Federação Bancária Europeia

Chief Executive of the European Banking Federation

PT

Quem está ligado ao sector bancário, sabe que lidar com criminosos é parte integrante do seu trabalho. Os bancos foram sempre um alvo apetecível e todos sabemos porquê: é onde está o nosso dinheiro. No entanto, a maior parte do dinheiro já não se encontra fechado em cofres protegidos por paredes espessas. Ao tornar-se virtual, o dinheiro passou a ser comandado por botões e armazenado em centros de dados (*data centres*), e a movimentar-se através de cabos de fibra ótica. Neste contexto, um ladrão de bancos moderno já não precisa de usar máscara ou arma. Hoje em dia, esconde-se por trás de um computador e usa *software* malicioso. Os cibercriminosos são, pois, os ladrões de bancos da era digital. Por essa razão, a cibersegurança não pode ser ignorada.

A revolução digital trouxe muitas oportunidades para o setor bancário e seus clientes, mas também novos riscos que devemos ter em consideração. Desde a criação dos primeiros serviços bancários *online* que os bancos têm estado na linha da frente do combate ao cibercrime. Felizmente, não estão sozinhos nesta luta. A cibersegurança é hoje uma prioridade na agenda política europeia e mundial. Em meados de setembro, a Comissão Europeia publicou o seu "Pacote de Ciber segurança", no qual elenca importantes propostas para a construção de uma União Europeia mais ciberresiliente.

EN

When you are in banking you know that dealing with criminals is part of the job. Because banks have always been a popular target and we all know why: because this is where the money is. However, most of our money is not any longer behind thick walls or vaults. As money is becoming virtual, it sits behind a button, moves around through fibre cables and is stored in data centres.

Accordingly, the modern bank robber no longer needs a mask or weapon. He now hides behind a computer screen and his bullets have become evil bytes. When it comes to banks, cybercriminals are the bank robbers of the digital age. It is clear that the need for cybersecurity cannot be ignored.

The digital revolution has brought many opportunities for the banking sector and its customers but also new risks to consider. From the onset of the first *online* banking services, banks have been at the forefront in the fight against cybercrime. Fortunately, banks are not alone in this fight; cybersecurity now has become a pressing issue on the political agenda in Europe, but also in the rest of the world. Mid-September the European Commission published its Cybersecurity Package outlining important proposals to build a more cyber resilient EU.

Outubro é também o Mês Europeu da Cibersegurança – um mês repleto de projetos e eventos promovidos pela Agência Europeia para a Segurança das Redes e Informação (ENISA). Enquanto parceiro da ENISA, a Federação Europeia de Bancos organizou no dia 10 de outubro a segunda edição da Conferência de Cibersegurança, sob o tema *"Managing Risk. Deploying Awareness"*. Este evento anual foi um sucesso junto do público e contou com um grande número de participantes. Um dos principais objetivos era fazer o ponto da situação da cibersegurança na indústria financeira e do trabalho conjunto que bancos, bancos centrais e outras autoridades (governo, reguladores, aplicação da lei) têm desenvolvido nas diferentes dimensões do problema. O êxito da conferência veio confirmar que a cibersegurança das instituições bancárias se tornou num tema extremamente relevante para todos.

Os desafios que os bancos enfrentam

Os crimes tradicionais não são novidade para o sector bancário. Porém, o cibercrime é mais complexo. Os ataques têm lugar em todas as frentes e são, amiúde, extremamente bem organizados. Os cibercriminosos são indivíduos muito inteligentes e criativos, e dispõem de um vasto arsenal de armas: *malware* (*software* maligno) *ransomware* (extorsão informatizada, baseada no resgate de informação armazenada por indivíduos, empresas ou outras organizações), DDoS (Ataques Distribuídos de Denegação de Serviço), *phishing* (envio de *emails* não solicitados para induzir o utilizador a fornecer dados pessoais e/ou financeiros), engenharia social, vírus, troianos. Conseguem, inclusive, pôr máquinas multibanco a 'expelir' dinheiro. Isto é real e a sofisticação dos ataques aumenta a cada dia que passa. Mais importante: o facto de o cibercrime não ter fronteiras faz com que seja um problema relevante à escala global. O recente ataque *WannaCry,* que afetou milhares de computadores em mais de 150 países, é apenas um exemplo.

October is also the European Cybersecurity Month, a month full of projects and events initiated by Europe's Agency for Network and Information Security (ENISA). As a close partner of ENISA, the European Banking Federation organised, on 10 October, the second annual Cybersecurity Conference *"Managing Risk. Deploying Awareness",* which turned out a great success with many attendees. One of the main goals of the conference was to show the state of play of cybersecurity in the financial industry and to discuss how banks, central banks and different authorities (government, regulators, law enforcement) are working together on different dimensions. The success of this event confirmed the fact that cybersecurity in banking has become an extremely relevant topic for all.

Challenges for banks

Traditional crime is not new for the banking sector. Cybercrime, however, is more complex. Attacks take place on all fronts, often in an incredibly well-organised way. Cybercriminals are extremely smart and creative people and have a wide arsenal to attack: malware, ransomware, DDoS attacks, phishing, social engineering, trojan viruses and can even make ATMs generate money at will. This is all real and it is becoming more sophisticated every day. But more importantly, let's be aware that cybercrime has no borders and this makes it an issue of global relevance. The recent WannaCry attack affected thousands of computers in more than 150 countries.

We see that throughout Europe many banks have their own cybersecurity practices. Some countries, such as the Netherlands and the United Kingdom have disaster exercises in place or national cybersecurity agencies to turn to. Partnerships between law enforcement and the financial sector have led to several operational successes in many countries in terms of prevention, intervention and prosecution of cybercriminals. But this is not the case in all countries.

“Uma ação coordenada começa pela partilha de informação e transmissão de conhecimentos técnicos, dados estatísticos ou detalhes específicos sobre métodos de ataque. ”

“Coordinated action starts with sharing information, getting everyone informed at the same time with expertise, statistical data or even specific details on attack methods. ”

Partilha de conhecimento transversal a toda a indústria

Uma ação coordenada começa pela partilha de informação e transmissão de conhecimentos técnicos, dados estatísticos ou detalhes específicos sobre métodos de ataque. Podemos aprender uns com os outros e acelerar a tomada de decisões. No nosso caso, promovemos iniciativas da indústria para a criação de plataformas de intercâmbio de ciberinteligência, ao mesmo tempo que trabalhamos em estreita cooperação com o Centro Europeu de Cibercrime (EC3), da Europol, para facilitar a comunicação com o sector. Como é evidente, a rapidez na partilha de informação sobre uma ciberameaça aumenta a probabilidade de as outras organizações protegerem mais rapidamente, e melhor, os respetivos sistemas. Porém, a partilha de inteligência ao nível das ciberameaças entre os *players* da indústria, as autoridades responsáveis pela aplicação da lei e outros *stakeholders* depara-se, muitas vezes, com obstáculos legislativos, na maior parte dos casos relacionados com o tipo de dados que podem, ou não, ser partilhados. A confiança é, pois, um elemento fundamental. A confiança não pode ser imposta por decreto, é algo que se constrói em conjunto.

Comunique esses incidentes!

Defendemos a necessidade de criar um sistema de categorização comum para a comunicação de incidentes. É neste contexto que a Federação Europeia de Bancos não só facilita a troca de informação e de práticas entre os seus membros, como mantém uma postura dialogante com supervisores e reguladores na UE. O enquadramento legislativo, tanto a nível europeu como nacional, introduziu requisitos de comunicação de ciberincidentes por parte das instituições bancárias. O que parece uma evolução positiva à primeira vista, esconde um sistema de comunicação complexo que obriga os bancos a comunicar um incidente às autoridades nacionais e europeias em prazos diferentes e usando informação heterogénea. Daí a necessidade de adotarmos um enquadramento legal consistente e harmonizado em todas as jurisdições e entidades reguladoras na Europa.

Sharing the knowledge industry-wide

Coordinated action starts with sharing information, getting everyone informed at the same time with expertise, statistical data or even specific details on attack methods. You can learn from each other’s experiences and make faster decisions. We promote industry initiatives to create cyber intelligence sharing platforms, while working closely with Europol’s cybercrime centre (EC3) to facilitate communication with the sector. Evidently, the quicker an organization can share information on a cyber threat, the more other organisations can protect their systems better and quicker. However, sharing of cyber threat intelligence between the industry, law enforcement agencies and other stakeholders often comes across legislative obstacles mainly related to the kind of data that may or may not be shared. Trust is an important component that needs to be created. We cannot legislate trust, only build it, and we must do that together.

Report those incidents!

We believe there is a need for a common reporting taxonomy and to this end the EBF facilitates the exchange of information and practices between its members and maintains a dialogue with supervisory and regulatory bodies in the EU. The European regulatory frameworks and various national legislations have introduced reporting requirements of cyber incidents by banks. At first sight, this is a positive development but it also has created a complex reporting grid where a bank must report an incident to national and European authorities, in different timeframes and with heterogeneous data. That is why we need a consistent and harmonised legal framework across all jurisdictions and different regulating entities in Europe.

“ Perto de metade da população europeia carece de competências digitais básicas, necessárias para nos protegermos *online*. ”

“Almost half of the European population lacks basic digital skills, which are necessary to protect ourselves once we go online. ”

Os seres humanos são o elo mais fraco

Na maior parte dos casos, os seres humanos são o elo mais fraco na prevenção de ciberataques. Perto de metade da população europeia carece de competências digitais básicas, necessárias para nos protegermos *online*. Pequenos erros podem ter consequências: usar a mesma palavra-passe em diferentes contas/acessos e descarregar atualizações de *software* são apenas dois dos exemplos mais comuns de simples medidas de proteção que ignoramos e nos tornam mais vulneráveis. A resposta a este problema passa pela sensibilização, daí termos como objetivo desenvolver as competências digitais de atuais e futuros clientes e colaboradores, mediante a promoção de iniciativas de sensibilização, designadamente em parceria com o EC3 ao nível das suas campanhas sobre lavagem de dinheiro, *ransomware* e *malware*. Também nos tornámos membros da Coligação para a Empregabilidade Digital, lançada pela Comissão Europeia, e estamos a trabalhar no sentido de incluir a literacia digital nas iniciativas de educação financeira realizadas no âmbito da *European Money Week*.

O que devem fazer os bancos?

Há três anos atrás, concluímos que era necessário unir forças ao nível europeu e que era tempo de países e organizações estreitarem a sua cooperação. Todas as ações levadas a cabo pela Federação Europeia de Bancos sublinham a necessidade de uma colaboração transfronteira, daí termos assinado um Memorando de Entendimento com a Agência Europeia para a Cooperação Policial, Europol, e trabalhado de perto com a sua unidade de cibercrime, EC3, com a ENISA, o FS-ISAC (*Financial Services Information Sharing and Analysis Center*) e outros atores na área da cibersegurança. Os resultados destas parcerias têm sido positivos, pelo que defendemos mais Parcerias Público-Privadas em todos os países. Os conhecimentos do sector privado podem ser úteis para outras indústrias e governos, a par das melhores práticas bancárias, que poderão ser usadas em todas as fases de criação, implementação, avaliação e análise de redes de cibersegurança.

É provável que o próximo ciberataque já esteja em curso, mas se mantivermos os nossos esforços de sensibilização e envolvermos todos os stakeholders, utilizando as ferramentas de segurança certas e as leis existentes, a indústria poderá preparar-se para estes desafios.

Humans are the weakest link

In most cases, the weak link in the prevention of a cyberattack are humans. Almost half of the European population lacks basic digital skills, which are necessary to protect ourselves once we go online. Small mistakes can have consequences; not using the same password for multiple accounts and downloading software updates are only two very common examples of simple safeguards that we ignore and thus make us all vulnerable. Creating awareness is the answer to tackle this problem. We want to enhance digital skills of existing and future customers and employees; hence we promote and create awareness-raising campaigns, notably with the EC3 and its campaigns on money muling, ransomware and malware. Also, we have become a member of the Digital Skills & Jobs Coalition of the European Commission and we are already working to add digital literacy to our financial education initiatives, during the European Money Week.

What is next for banks?

Three years ago, we saw the need to join forces on a European level and believed it was time for organisations and countries to work more closely together. In all our work at the European Banking Federation, we stress out the need for cross-border collaboration. That is why we signed an MoU with European law enforcement agency Europol and work closely with its cybercrime unit EC3 but also with ENISA, FS ISAC and other actors in the cybersecurity field. And we see the positive results of these kind of partnerships. Therefore, we must aim for more Private-Public Partnerships (PPPs) in all countries. The insights from the private sector can benefit other industries and governments. Best practices in banking can be used for all the stages of creation, implementation, evaluation and review of cybersecurity frameworks.

The next cyberattack is probably already on its way. But if we keep raising awareness and involve all stakeholders, with the right security tools, rules and governance in place, the industry can be prepared.