bobsguide
Connecting buyers and sellers of financial technology globally

The cybersecurity risks to financial services that are making the biggest impact in 2017

21 August 2017

Cliff Moyce, Global Head of Finance Practice at DataArt, details the security trends that should currently be giving financial services executives the biggest headaches.

Your ability to respond

Cybersecurity products and platforms can do a great job for you—when your organisation has the expertise and number of people needed to implement and use them correctly, for example, to configure and tune the products and interpret the large volumes of data being produced. The problem for most firms involved in financial services and capital markets is that they just don't have the number of people or the skills and experience required to use their tools well.

A series of reports from Cisco, Symantec and Cybersecurity Ventures has estimated the likely future shortfall in cybersecurity talent, with the latter firm estimating there will be 3.5 million unfilled cybersecurity jobs by 2021. When financial services firms try to fill this skills gap by hiring consultancies, they often find that the consultancy is more interested in selling licences for their own toolset rather than giving the required man-hours to protect daily operations. Some cybersecurity product firms have added consulting arms in recent years, but it is unlikely (read: impossible) that this can be enough to fill the current gap, let alone what is coming.

The security talent shortage means that top talent is difficult to hire. The people you need will not be looking for a job, and most will be loyal to what they are doing now. How are you going to make the cyber-security challenges at your financial services firm attractive enough to tempt the best people? For a start, firms need to take the people issue seriously; they need to forget about hiring restrictions, preferred geographies and pay parity etc; in the same way that they need to forget the idea that cyber threats can be neutralised with software only. The people that are a threat to their companies laugh at most IT security products (see #2 ‘Professionalisation of cyber-crime’, below) and so should the people you hire. Remember, the cost of failure in cybersecurity can be huge. You need people who are verifiably expert (and recognised as experts – not just people with well written cv's) in defending against all known attack types, such as denial of service; eavesdropping; backdoor; direct access; zero-day; and, supply chain attacks. You also need people who are expert in malware, botnets, ransomware and all the other tools of the trade. And you need people who understand how cyber-crime operates in 2017 (again: see #2: Professionalisation of cyber-crime').

Professionalisation of cyber-crime

These days most malicious hacking attacks against corporations originate from professional, organised groups. Attempts by the media to conflate the money-making enterprises perpetrating the attacks to certain geographies or political ideologies can be unhelpful and cause confusion. Be under no illusion: these people have come for your money, not your votes.

Cyber-security is no longer a cottage industry. Usually, it is not just one organisation that is effecting the whole crime. Specialisation is the name of the game. Syndicates building tools for cyber-theft are rarely the same people as those who are using them to steal money. Not only does this syndication of loosely attached, dispersed organisations make it harder for law enforcement agencies to disrupt criminal activities, but the specialisation also plays to different strengths of individuals. People who get pleasure from the technical and intellectual challenge of building tools that can penetrate and replicate within corporate and global networks while unseen and undetected, are different sorts of people from those who want to steal money: but make no mistake – both are involved in a criminal conspiracy. Even within an 'organisation' that builds tools only, one team might be dedicated to creating malware; another will be creating botnets; and, another will set up and maintain distribution channels (eg renting out botnets), etc.

But more important to firms in financial services and capital markets is the fact that professionalization of cyber-crime is a paradigm shift against which most common corporate security defences are ineffective. This is because most commercial IT security tools (anti-virus, anti-malware, firewalls etc) are based on assumptions that are no longer valid i.e. they were designed to dissuade the lone amateur hacker, or a small group of amateur hackers, not large criminal organisations. When a criminal organisation is run as well or better than the organisations they are targeting, then those targets are in trouble. Financial services organisations doing more of what they do now will not be enough, even if they do it better than they did before. Those organisations need to change how they think; most importantly they need to understand how professional cyber-criminals are thinking. This is where working closely with global policing and security agencies such as Interpol, the FBI, and GCHQ can be useful.

Erosion of trust

Retail clients of financial services and e-commerce are tired of the constant threat from small scale, high volume, medium impact crimes coming from phishing, vishing and smishing for user-names, passwords, credit card details etc. When every family has at least one member who has lost money to such scams; attempts are being made on a daily basis; and, the press runs articles constantly on banks not recompensing customers for losses, it is no wonder that customer satisfaction with banks is not rebounding as it should have done post financial crash. In short, financial services is not regarded as being secure from cyber-crime. And there is good reason for this – it is not secure.

Unfortunately, there is an industry of small operations set up to benefit from these high volume, low value thefts. If more could be done to tackle the industry of money laundering operations that support cyber-theft then trust could start to be restored. It is not hard to find the money launderers. There are thousands of them competing to take a cut from internet criminals, and they are advertising their services openly with phrases such as "no questions asked.” They can be found easily on public bulletin boards; this is not a ‘Dark Web’ activity. The more that can be done to disrupt the infrastructure that supports cyber-criminals, the better for the industry. Financial services and police forces worldwide need to work together to make this happen.

Original article can be found here: http://www.bobsguide.com/guide/news/2017/Aug/21/the-cybersecurity-risks-to-financial-services-that-are-making-the-biggest-impact-in-2017