When cybercrime met big business

Healthcare

In the past two to three years, my perception of the typical cybercriminal has shifted. They might not be 'suited and booted' but, in my mind, he or she is nevertheless a business person running an efficient operation, complete with a clearly defined business model and strategy.

In the past two to three years, my perception of the typical cybercriminal has shifted. They might not be 'suited and booted' but, in my mind, he or she is nevertheless a business person running an efficient operation, complete with a clearly defined business model and strategy.

It's an important change of perception. To persist with thinking of the typical cyber criminal as a solitary, tech-savvy hacker, operating from home, pursuing ideological or anarchistic objectives, is to diminish how much of a threat they pose.

That used to be the reality of the situation; lone raiders who were technologically proficient in one kind of cyber attack tool, looking to exploit that tool for maximum effect. That's changed now.

In that person's place has come a cyber criminal CEO who treats each job differently, using whatever tools and skills best suit it. If they don't have those tools and skills to hand, they will go and purchase them from the market on the dark web. They will have a strategy. They know what assets they are after, how to monetise them and how to launder the proceeds. A slick and efficient operation. It's highly organised crime in a digital world.

Listen to that language again. Tools, skills, market, strategy, assets. This is corporate terminology we're using here.

Why does that matter? Because to understand an opponent's motivation is to understand how best to defend ourselves.

The most dangerous attacks nowadays are not random acts of petulance; they're serious business undertakings, designed to extract maximum value from a target. In fact, a recent KPMG and BT report suggested that 89% of cyber-attacks now have a financial or espionage motive.

This is not a contest between our businesses and geeky hackers. This is business versus business and to best protect ourselves, we must begin thinking in the same way as if our organisation came under a legitimate threat from a competitor.

They won't bother with us, will they?

Although we might prefer to think otherwise, the healthcare sector is most definitely at risk from this sort of attacker. In terms of a league ranking of attractive sectors, I'd have it squarely in the middle of the pack – but rising.

The financial services sector remains the clear #1 target because it's flush with cash. Further back down the field - but advancing rapidly - stand retail (awash with personal details and bank transactions), manufacturing (a highly liquid sector with a complex supply chain) and even professional services (often a handy back-door route into other, more lucrative targets).

Healthcare sits in this group too – and understandably so. There are millions of transactions taking place across its highly fragmented supply chain. There are suppliers to be paid, large numbers of agency staff to be employed and expenses to be processed; representing thousands of potential attack points.

© 2016 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

A prime target here – but not the only one – will be the healthcare sector's data, which is a rich data set indeed. As with any sector, healthcare businesses will hold information on R&D projects, collaborations and potential acquisitions; all of which can be market sensitive. However, the vast amount of personal data which it holds looks even more attractive.

Medical records are hugely valuable, providing a cybercriminal with all the information required for classic identity theft. Accordingly, such records are traded on the grey market at prices far in excess of those charged for stolen credit card details for example. Health insurers have already been targeted for exactly this reason. It seems logical to expect that mainstream healthcare providers will be targeted with the same motive.

Although some data hacks will still be perpetrated primarily for purely disruptive reasons, most such attacks do now have a commercial motive. Identity theft remains a possibility but extortion features far more prominently as the rewards here could be far higher.

Threatening to embarrass high profile individuals by releasing extremely personal medical records might be one avenue. Another may be demanding that an organisation pay a ransom to avoid losing all its hard-earned data and suffer the reputational ignominy of public censure.

I'm not sure that this threat features too prominently in the public consciousness just yet though. They'll be fearful of identity theft and they'll hear occasional stories of data mishandling. The threat of malicious criminal intent does not feature on their agenda – or, seemingly, the media's.

For example, the extensive coverage of the recent WADA hack, seemingly undertaken in an attempt to seek revenge for the banning of Russian Olympic athletes, appears indicative of how the media pays far more attention to the ideologically-inspired cyber attacks than their criminally-inspired counterparts.

Hands up – and phones down

I mentioned that healthcare data is an attractive target for cyber criminals – but so too are healthcare sector IT systems. As healthcare becomes more digitised, so too does the scope for denial of services attacks.

For example, hospitals may be at risk from Telephony Denial of Services (TDoS) attacks which see their systems swamped by bogus phone calls. Such an attack can cripple an organisation's ability to take appointments, track and treat patients. This is classic extortion-with-menaces territory; "pay what we ask for if you want to get back in business".

© 2016 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

In the worst case scenario, an organisation's entire IT estate could be taken out of action. As it begins to break down and functionality is lost, the temptation to accede to the criminals' demands would grow ever greater.

And this is where some of my biggest fears for healthcare lie. Legacy IT systems, historic under-investment, 'flat' networks with insufficient internal security controls; factors like this leave the sector exposed to attack.

To further complicate matters, this is a very decentralised industry. Primary and secondary care providers of all shapes and sizes, inextricably bound up with private sector suppliers, operate in a sector with few regulatory obligations around cyber security. Yes, the NHS is coming under some pressure to consider how to secure the sector. In turn, this may cascade down the supply chain but private sector suppliers may not feel obliged to sit up and take notice until there is a very real threat to their own profile and reputation.

My biggest fear however stems from the agility of the modern day cybercrime business people. The speed with which they can experiment and innovate is frightening. Stacked up against that, we have healthcare security programmes which are typically driven primarily by compliance, not innovation.

Inflexible bureaucracy and the inertia of legacy systems compromise our ability to react flexibly. Together they represent the sector's biggest vulnerability.

So far, so bleak.

It's tempting to think of this as an unfair fight; the smart, tech savvy business operator, with no regard for the rule of law, up against the hide-bound behemoth sector, constrained in its ability to invest in its defences as fully as it would like.

That's not strictly true. For a start, facing down the threat of some of the more commoditised attacks (phishing, ransomware, watering hole attacks etc.) can be achieved simply by getting some of the basics right from the Cyber Essentials scheme, especially if this can be done centrally as part of a managed security system.

I can imagine a stratification of defence mechanisms coming into play here. The basic stuff, done properly by organisations, collectively or individually, overlaid by a number of more advanced, government sponsored, services and topped off by government plans for proactively disrupting the criminals themselves. Certainly, I think that government has a big part to play here and is slowly realising that the smaller organisations need their help and guidance just as much as the larger ones do.

My main pieces of advice would therefore be as follows. Firstly, establish the cyber security essentials. Secondly, consider investing in educating your staff, raising awareness of the types of threat you face and the dangers they can pose. Forewarned really is forearmed. And thirdly, plan for – and simulate – the cyber-attacks which could cause you most danger.

This third point will require you to consider how you deal with such attacks, what your ransom policy is and the point at which you get the police involved. Like a traditional business continuity plan, you'll need to determine how you'll be able to maintain or restart business as usual and how best to communicate with affected parties, most notably patients.

All of which brings us neatly back to thinking about your opponent as a business person. To determine what the most dangerous cyber threat to your organisation is, consider what that rival criminal business person will most want from your business. Stop thinking solely about technological defences and start thinking strategically. Rather than only trying to make that desired data or outcome harder for them to secure, how can you make it less appealing and less valuable?

Quite simply, seek to minimise the potential return on their investment of time and effort. Your potential opponent knows how high the stakes are. They are not in this for kicks and they certainly will not persist in their efforts if the pay-off is not worth the risk. Think about how you put them out of business.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The views and opinions expressed herein are those of the interviewees and survey respondents and do not necessarily represent the views and opinions of KPMG LLP.

© 2016 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.
CRT071395 | November 2016

David Ferbrache

Technical Director
Cyber Security
KPMG in the UK

Share your views and join the debate:

Visit us
kpmg.com/uk/healthcare

Email us
publicsectormarketing@kpmg.co.uk

Engage with us
Follow us on Twitter @
KPMGUK