KPMG

BT

Taking the offensive:

Disrupting Cyber Crime

Rethink the cyber security threat

01

As the threat of cyber attack grows, major corporations are struggling to keep pace with the tactics of criminal gangs, hacktivists, less ethical governments and even, perhaps cyber terrorists.

All boards have become aware of the importance of robust cyber defences, sometimes, and painfully, after the event. But at a time when attackers are moving so quickly, the traditional approach to security is no longer fit for purpose. A new way of thinking is required – one which starts from the mindset of the attacker.

"Nearly a third of CEOs list cyber security as the issue that has the biggest impact on their company today, yet only half feel prepared for a cyber attack."

KPMG Global CEO Outlook 2015

300 MILLION

According to one anti-virus vendor (Symantec), over **300 million** distinct examples of malware are created in a single year

Ruthless and rational entrepreneurs

02

The twenty-first century cyber criminal is a ruthless and efficient entrepreneur, supported by a highly developed and rapidly evolving black market. Like any entrepreneur, the cyber attacker's intention is to make money – fast.

Criminal groups who mount a constant assault on legitimate businesses are not simply members of an amorphous underworld: they are, in fact, operated as rational hard-nosed businesses, with their own clearly defined business models and money making scams. While the modus operandi might be information theft or blackmail underpinned by the threat of denial of service, it is ultimately about making money at the expense of the target organisation and its customers. And while these cyber entrepreneurs are undoubtedly criminals, they are akin to competitors who are intent on disrupting your market.

However, unlike conventional competitors, cyber-crime entrepreneurs do not play by the rules. Not only are they ruthless in pursuit of their goals, they are also unencumbered by laws and regulations; perfectly content to damage the organisations they attack and exploit the customers who are often the ultimate victims. Criminal organisations also don't seem to have liquidity issues - they appear to have cash ready to invest in developing attack tools and finding vulnerabilities in corporate information systems - perhaps hiring or buying what they need from a growing army of cyber black marketers.

This shadow market is a hotbed of R&D. In an internet economy that is worth over $4 trillion, many commentators put the losses from cyber-crime in the $100s of billion worldwide per annum. The profits made by criminal entrepreneurs ensure that new attack tools are developed at an astounding rate. This is manifest in the sheer number of malicious software products in the wild. The profligacy of software development is matched by operational efficiency. Witness the astonishing speed at which traffic from hundreds of thousands of computers can be marshalled in denial-of-service attacks against our corporate web servers.

The threat is not solely external. Criminal entrepreneurs are quite prepared to plant people inside major organisations, blackmail or bribe employees. They are happy to breach the security of suppliers in order to reach their ultimate target - you. To add insult to injury, sometimes they even end up competing for the same talent as legitimate businesses. And they don't respect our neat definitions of insiders and outsiders; physical, personnel and IT security.

169 MILLION

... identities were stolen in 2015, according to statistics gathered by the Identity theft research centres (ITRC)

Shadow markets and black economies

02

It is hard to underestimate the power of cyber criminal entrepreneurs. They head major transnational organisations and, in the eyes of the authorities, they are key targets for law enforcement. Witness Evgeniy Mikhailovich Bogachev, believed to be behind a vast operation to steal and exploit bank details using sophisticated malware. He is now riding high on the FBI Most Wanted list commanding a $3 million reward. Traditional businesses face asymmetric warfare, in which agile attackers operate outside the rules and deploy continually evolving tools and strategies to attack their targets on battlefields of their own choosing. These are organised and purposeful.

90 PERCENT

In the UK – one of the prime targets for cyber attack – a recent report by The Department for Business, Innovation & Skills (BIS) found that **90%** of large companies had suffered a security breach.

Taking the fight to the attackers

03

Businesses are struggling to keep up with cyber attackers, not least because conventional procurement cycles are failing to keep pace with the efficiency of the shadow market. A change in approach and mind-set is both required and long overdue.

The criminal entrepreneurs behind cyber attacks share some similarities to challenger brands. Both are trying to disrupt business models of successful companies; both are agile; and both are using technology as the catalyst to deliver their desired outcome. Both can vanish and reappear in a new form just as you are adapting to the original challenge. The difference is that successful companies do not sit back and simply allow their businesses to be disrupted– quite the opposite. Successful companies take steps to understand emerging competitors, in terms of their business models and technology.

Businesses should take the same approach to cyber criminals that they take to competitors and understand:

- Who the attackers are
- What they are setting out to achieve
- How they make their money

Once we know their business model, we should take steps to disrupt it, making it as difficult as possible for the criminals to go about their work. Or, put it another way, you make it more difficult for the attackers to monetise information theft.

The first line of defence is to keep criminals out of information systems. But breaches can and will occur, there are no perfect defences. We need to make it much more difficult for the attacker to use the information once they are inside the system – taking steps to detect and respond to intrusions, protecting key data using encryption and additional security, diverting and trapping attackers, and using new technologies to make sure our systems are constantly purged of any malicious code. If information is stolen, organisations should make it harder for cyber criminals to exploit it. Banks have led the way on this, thanks to increasingly sophisticated fraud control measures and constant monitoring to detect unusual activity, it is now much harder to use stolen credit card data.

In other words, cyber defences should extend beyond the prevention of systems breaches, to a wider range of anti-fraud measures aimed at making it much harder and more expensive for the criminals to use the information they procure or trade. Perhaps we'll see organisations bring together fraud control and cyber security functions and stop treating cyber security as just being about the protection of corporate IT systems in a world where boundaries are vanishing.

Expect criminals to disrupt your supply chain. Maybe it is time we did the same, ramping up our efforts to disrupt their infrastructure. It is unlikely that these proactive measures can be taken by individual corporates alone but together, and with law enforcement agencies, there is much more which we can do to take the fight to the criminals.

$400 BILLION

Annual cost of Cyber Crime – **$400 Billion**
Intel Security

The need for speed and agility

04

To succeed we also need our own cyber security organisations to be as creative and agile as their opponents. Given the pace of R&D in the hyper-efficient shadow economy, businesses will also have to harness innovative technologies and approaches.

When our national security is threatened, nations create unusual teams such as the British code breaking centre at Bletchley Park. These teams thrive on a culture of creativity, a drive to deliver, and a tolerance for radical thinking and diversity. A similar approach and urgency is needed when companies take on the challenge of cyber-crime.

Organisations should also be looking at how to source innovation from the marketplace, through partnerships and by setting up incubator programmes designed to attract and fund startups and early stage companies offering cutting-edge solutions. There are people issues too: to match innovation in the black market, companies should be prepared to grant more licence to their teams to innovate, and be ready to tolerate people who are just a little different and unconventional.

More broadly, we need to rethink our approach to risk and compliance. Traditional compliance processes seem out of step with the new digital age – and adding more and more controls at the cost of flexibility and agility only increases not reduces risk.

The digital opportunity and how to exploit it

05

Digital risk and opportunity are two sides of the same coin. Throughout every industry, digital innovation is creating new opportunities to drive efficiencies, serve customers better and increase profits. But that innovation can bring risk.

The challenge is to develop a digital business model that is resilient to cyber attack and that requires a strategy which looks at the digital risks facing the totality of the business – not simply corporate information systems – but critically customers and supply chains. This calls for a strategic approach that builds agility, as well as a responsive approach to digital risk in the business. It will be counter-cultural. Over years, companies develop processes that become, if not set in stone, certainly hard to change.

The reward for a flexible and holistic approach to cyber security is not just protection, but is the creation of sustainable competitive advantage. By successfully addressing risk, businesses are able to safely harness innovation.

A new role may emerge – the Chief Digital Risk Officer working closely with digital teams (and Chief Digital Officers) as new services are developed. This will be a strategic role. The Digital Risk Officer will have the technical skills needed to fulfil a security brief – including an understanding of big-data analytics – but critically they will also have an instinct for how attackers think. They are not there to say no – they are there to find a way to say yes to exploiting digital opportunities quickly and securely.

The cyber threat has never been more acute. In face of questioning from boards, shareholders, the media and analysts, businesses are naturally focused on how much cyber assurance is required.

The answer to that question will come in no small part from a new generation of digital risk professionals, monitoring and responding to attacks. But most of all genuine risk management comes from knowledge of your attackers, and an agile response which facilitates opportunity.

For more information please contact:

Ramy Houssaini
VP BT Security Europe
+33 (0) 695 697 229
ramy.houssaini@bt.com

David Ferbrache OBE
Technical Director, Cyber Security, KPMG
+44 (0) 131 527 6660
david.ferbrache@kpmg.co.uk