The changing face of cyber threats

March 2018

Digital business is a major enabler to building customer trust and investor confidence. If cyber security is poor, all efforts at digital transformation will be undermined.

Industry and governments are now in an arms race with professional criminal gangs and other nation states that are highly adept at deploying sophisticated tools and techniques designed to steal data and cause major disruption to the day-to-day running of major businesses, organisations and national communications infrastructure.

> "Any criminal with a brain is a cyber criminal."
>
> **Mark Hughes,**
> President BT Security,
> September 2017

> At BT we detect 100,000 malware samples every day – more than one per second – and we protect ourselves against over 4,000 cyber-attacks daily.

Much of the discussion around cyber security now focuses on espionage – states attacking other states using cyber techniques – and, to a lesser extent, hacktivism – ideologically motivated attacks.

Cyber lends itself very well to espionage techniques, allowing countries and major state-sponsored actors to infiltrate physically-secure spaces. Countries now include cyber techniques as part of their modern warfare arsenal.

Whilst these risks remain significant, the issues have moved on to the continual growth of cyber crime. We believe this to be a more pervasive and insidious challenge with a deeper impact on business and society.

Forecasts show that the number of connected devices will grow from around 27 billion in 2017 to 125 billion in 2030 as the Internet of Things grows in scale and importance. This, combined with the flow of digital business to the cloud, gives criminals many points of attack.

Criminals today are trying to take the currency of our age: data. This is happening at a faster pace and with greater sophistication than ever before.

Types of cyber attack

We use three broad titles to define the main methods used by cyber criminals:

1. Cyber theft for financial gain

Criminals seek personal details in order to steal money. In the UK, half of all reported fraud is now committed through cyber crime, with half of Britons having already been targeted.

Phishing is a popular method. In the last twelve months alone, we have identified and closed down more than 5,000 phishing sites.

Whaling (where criminals impersonate senior people in order to assume and abuse their authority) is becoming more popular.

2. Cyber vandalism: a desire to break things or disrupt

The most popular method is Distributed Denial of Service (DDOS) attacks where thousands of computers are used to take down websites.

The financial and reputational damage of such attacks on banks, governments, airlines, utilities, health providers and retailers can be devastating.

These attacks are daily occurrences for our customer-facing websites and TV platforms with our security team seeing more than 50 high alerts on average every day.

They are growing in frequency and size. We are already experiencing attacks of up to 650Gps.

3. Cyber extortion: using people's reliance on data and technology to hold them to ransom

With ransomware now available on the dark web for as little as US$50, criminals can enter this rapidly growing market very easily.

We have recently seen the WannaCry and Petya attacks spread across the world. Perhaps one of the most worrying aspects of WannaCry was how unsophisticated it was. Its vulnerability was well known and a patch was readily available.

Our recommendations

A lot of the vulnerability from these sorts of attacks comes through organisations not getting the basics right:

- updating anti-virus software
- investing in staff cyber-security training
- being distrustful of opening suspicious emails or links.

It's a public policy imperative that such disruption and targeting is prevented.
Our recommendations are:

1. **Invest in the latest technology** – in the form of firewalls, filters and AV software. This is important, but cannot solve the problem alone.
2. **Put cyber security at the top of the boardroom and country leadership agenda.** It is at BT. Make sure everyone in the organisation, from the board down, takes responsibility for maintaining high standards of cyber-hygiene.
3. **Implement a robust cyber security strategy.** Policies should be kept under constant review, continuously updated and put to the test. Cyber-savvy firms prepare for unexpected events.
4. **Invest in regular staff training.** This can help transform employees from being the weakest link in the cyber-security chain into every company's greatest asset in the fight to protect data.
5. **Employ ethical hackers to help bolster a company's defences.** Attack the company from the inside to unearth hidden vulnerabilities. This includes full-scale 'war games' where scenarios are played out in front of the executive team and board to test their response to a cyber crisis.
   - Build resilience and 'muscle memory'. At BT, we regularly hold 'Black Swan' exercises and scenarios that challenge so-called 'red teams' of ethical hackers to penetrate our defences against the 'blue teams' protecting the network.
   - We offer ethical hacking to our corporate customers, with dedicated ethical hacking services for specific sectors such as automotive (connected cars) and financial services.
6. **Move to the cloud.** Understand where your critical and sensitive data is located; manage identity consistently; and make sure you have the same level of compliance and data protection from your cloud services.
7. **Enhance cyber operations with big data.** Security, network, and user devices now produce vast quantities of data. You need to be able to rapidly make sense of that data; in real-time, to detect and prevent internal and external threats.
8. **Consider compliance as more than a box ticking exercise.** Take a fresh look at your entire security landscape and understand that agility matters. As threats and opportunities evolve, security needs to adapt, too. It's less about process and compliance, and more about being agile.

More action is needed

These initiatives are important, but digital criminals play to win. Too many organisations are working with fragile and insecure cyber-security defences that cannot support digital ambitions and allow digital criminals to outpace them.

Criminals and unfriendly governments are constantly evolving the sophistication of their attacks, and no technology can fully overcome the incidence of human error.

Organisations need to be proactive. No security is permanently impenetrable to a skilled and determined criminal. If they are able to exploit vulnerabilities before they are publically disclosed, or change malware and botnets as soon as they are detected, an organisation can get caught in a game of catch up that it's destined to lose.

The most effective protection lies in taking the fight to the attacker by deploying security tools, procedures and strategies that make it more difficult and costly for criminals to operate.

This includes:

- a multi-layered approach
- protecting information with encryption
- systems to limit the scope for using stolen data
- partnerships with peers. Build a community: think about a blend of building relationships with your peers, formal sharing platforms and maybe even commercial threat feeds. Be prepared to share what your organisation is seeing and seek to get involved.

On this last point, and counter to culture, we strongly believe that companies and organisations need to learn to share experience and lean on others, because whatever is done alone will never be enough. The time is ripe for companies – and ISPs in particular – to work more closely with governments to help neutralise cyber crime.

BT and cyber security

- We operate one of the world's largest networks, extending across 180 countries – including the largest fixed and mobile network in the UK.
- We provide services to millions of customers – households, businesses, governments and entire nation states – who trust us to protect their data.
- We help our customers to thrive in the digital world by delivering world-class security solutions through over 2,500 security professionals operating from 15 Global Security Operations Centres – making us one of the largest dedicated security practices in the world.
- Over the past two years, we have seen a 1,000 per cent increase in the volume of threats directed at our networks and our customers' networks. We have stepped up our security investment and are taking an intelligence-led, proactive approach to identifying the increasingly global threats that we are seeing across the network. By spotting any attacks and vulnerabilities rapidly, we are able to speed up our response and take the most appropriate course of action.
- The lessons that we have learned through defending our own network from attacks combined with our global reach and depth of expertise, gives us unparalleled insight into the cyber landscape.
- Cyber crime is a rapidly-expanding market that requires little resource and risk on the part of criminals to enter. Security specialists like us need to continue to innovate in this space to help stay one step ahead of today's ruthless cyber crime entrepreneurs. We are constantly watching, learning, predicting and responding to the latest threats set by the cyber criminals and unfriendly governments and their actors.
- We protect not only customers' and our own infrastructure, but also the UK's critical national infrastructure. Other countries are starting to entrust the security of their critical national infrastructure to us, too.
- We provide managed security services to over 1,000 customers worldwide, including both FTSE100 and Fortune 500 companies – perhaps our greatest recommendation.

For further information please contact Stephen Crisp, VP Public Affairs, Asia, Middle East and Africa, BT.

stephen.crisp@bt.com

Offices worldwide
The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

Registered office: 81 Newgate Street, London EC1A 7AJ.
Registered in England No: 1800000.