Trends in cybercrime

In the “Internet Organised Crime Threat Assessment” report published in the course of 2018, Europol highlighted some recent trends in cybercrime:

- Cybercriminals used ransomware (such as the “WannaCry” attack) to target private companies and obtain a ransom in exchange for the release of certain parts of their data.
- Distributed-Denial-of-Services (DDoS) attacks become low cost, and easier to deploy.
- Even though geo-blocking measures have decreased this kind of cybercrime, skimming of payment cards is still a common issue in the EU.
- Criminals continue to rely more and more on social engineering in order to carry out their cybercrimes.
- “Phishing” and “spear phishing” are widespread.
- New types of cybercrime have emerged such as “cryptojacking”, which consists in exploiting an internet user’s bandwidth and processing power to mine cryptocurrencies.

Looking ahead, experts expect:

- The dual use of artificial intelligence (e.g. both as a cyber threat as well as a cyber security defence mechanism).
- The multiplication of risks due to the increasing use of internet of things technology and machine to machine communications and the increasing collection of more and more data.
- The use of “deep fakes” to deceive, blackmail and spread fake news.
- The expanding involvement of state-sponsored actors.

Impact

High profile cases: A recent Linklaters report identified a 50% increase in large data breach incidents over the last three years. Last year, high profile cyber security incidents included the access by hackers to around 30 million Facebook accounts and the breach of security involving 500,000 Google+ accounts. These cases tend to have an increasing impact on the stock price/valuation of the relevant companies and the tenure of senior management.

Legislative actions: In 2018, many countries have adopted new provisions regarding cyber security. EU Member States were due to transpose the NIS Directive by 9 May 2018 and identify the covered operators of essential services by 9 November 2018. Asian countries including China, Singapore and Vietnam, adopted cyber security legislation, while others such as India and Australia adopted (amendments to) data protection rules with cyber security implications.

Regulatory cooperation/standards: In the EU, the NIS Directive and other instruments support strategic cooperation and exchange of information among countries through the creation of a cooperation group and a network of computer security incident response teams. A political agreement was reached on the cyber security act in December 2018, aiming to strengthen the European Union Agency for Network and Information Security by granting it a permanent cyber security mandate and allocating more resources to it. It also creates a framework for European Cyber security Certificates for products, processes and services that will be valid throughout the EU.

Complexity of new actors: Cybercrime is not limited to lone wolf and financially motivated crimes. A range of state actors worldwide also engage in cyber warfare, be it for political and/or strategic objectives or for financial motives.

Impact of the EU’s GDPR on policy-making worldwide: An increasing number of countries outside of the EU are aligning their data privacy laws on the EU model, including the introduction of mandatory data breach notifications (rendering cyber security incidents more visible) and increasing fines. For example, New York’s Stop Hacking and Improve Election Data Security (SHIELD) Act, intended to modernize New York’s current data privacy laws, is pending before the New York legislature.

Linklaters has one of the longest-standing privacy and cyber security teams and clients benefit from our experience, over many years, of advising on some of the most serious hacking and data breach crises in the last decade. If your organisation is facing a serious cybercrime issue or wants to ensure you are prepared to handle a cyber incident, please contact one of the following members of the Linklaters global crisis response team:

- Tom Cassels
  Partner, London
  Tel: +44 20 7455 3755
tom.cassels@linklaters.com

- Richard Comley
  Partner, London
  Tel: +44 20 7456 3750
richard.comley@linklaters.com

- Daniel Pady
  Partner, Frankfurt
  Tel: +49 69 710 03 820
daniel.pady@linklaters.com

- Adam Lurie
  Partner, Washington, D.C.
  Tel: +1 202 654 9227
adam.lurie@linklaters.com

- Richard Cumbley
  Partner, London
  Tel: +44 20 7456 4681
richard.cumbley@linklaters.com

- Adrian Fisher
  Counsel, Singapore
  Tel: +65 6692 5856
adrian.fisher@linklaters.com

- Daniel Pady
  Partner, Frankfurt
  Tel: +49 69 710 03 830
daniel.pady@linklaters.com

- Tanguy Van Overstraeten
  Partner, Brussels
  Tel: +32 2 501 94 05
tanguy.van_overstraeten@linklaters.com

Linklaters LLP is a limited liability partnership registered in England and Wales with registered number OC326345. It is a law firm authorised and regulated by the Solicitors Regulation Authority. The firm partners in relation to Linklaters LLP are members of the LLP and are not partners in the sense that term is used in connection with a partnership of registered foreign lawyers. Please refer to www.linklaters.com/regulation for important information on our regulatory position.
Cyber security: Global status and trends.

**U.S.:** Clarifying the Legal Overseas Use of Data (CLOUD) Act grants U.S. law enforcement increased access to U.S. data stored overseas by U.S. service providers. UK-U.S. negotiations underway to sign a bilateral agreement to facilitate law enforcement data sharing.

**U.S.:** California Consumer Privacy Act passed in July 2018, will impose “GDPR like” privacy obligations on businesses and affiliated/co-branded entities possessing personal information on California residents (if thresholds are met).

**U.S.:** Growing enforcement area for U.S. regulators including the SEC, which recently warned publicly-traded companies to protect against cyber-attacks or risk internal controls violations.

**Brazil:** Newly adopted data protection law requires security measures to ensure protection of personal data and requires breach notifications to regulator and individuals.

**Argentina:** New guidelines from Agency of Access to Public Information allow multinationals to use binding corporate rules (BCR) for cross-border personal data transfers within the group.

**Worldwide:** Google closes its social network, Google+, after disclosing a data leak potentially affecting 500,000 Google+ accounts.

**UK:** Fine of £500,000 imposed by ICO on Equifax Ltd (under the old, pre-GDPR law) for failing to protect the personal data of millions of individuals, including up to 15 million persons in the UK.

**EU:** From 2019, Payment Services Directive (2015/2366) requires payment service providers to apply stricter security rules on authentication (including a two-factor-authentication).

**EU:** From 2019, Payment Services Directive (2015/2366) requires payment service providers to apply stricter security rules on authentication (including a two-factor-authentication).

**U.S.:** Fine of £500,000 imposed by ICO on Equifax Ltd (under the old, pre-GDPR law) for failing to protect the personal data of millions of individuals, including up to 15 million persons in the UK.

**EU:** From 2019, Payment Services Directive (2015/2366) requires payment service providers to apply stricter security rules on authentication (including a two-factor-authentication).

**Worldwide:** Google closes its social network, Google+, after disclosing a data leak potentially affecting 500,000 Google+ accounts.

**Australia:** Privacy Amendment (Notifiable Data Breaches) Bill 2016 in effect since February 2017 with mandatory data breach notification.

**Australia:** Telecoms and Other Legislation Amendment (Assistance and Access) Bill 2018 tabled to enable security/law enforcement access to encrypted communications or devices.

**Belgium:** Prosecution of drug traffickers who hacked the IT systems of two companies operating in the port of Antwerp to locate and steal containers containing drugs.

**Germany:** Federal Office for Information Security recently urged companies to invest in adequate security measures due to the increase in cyber-attacks on German companies.

**Germany:** First GDPR fine imposed on a social media company for lack of IT security (plain text passwords stored), resulting in a September 2018 breach which affected 330,000 users.

**France:** Law adopted to fight manipulation of information, ie “fake news”, due to concerns over online misinformation campaigns, eg to influence the outcome of elections.

**China:** The Chinese Cybersecurity Law came into effect in June 2017. Key features include obligations to notify data breaches and restrictions on cross-border data transfers.

**Vietnam:** Law on Cybersecurity effective as of 1 January 2019 gives extensive powers to the state and contains data localisation requirements, among other obligations.

**Singapore:** CyberSecurity Act of 2018 aims to strengthen protection of “Critical Information Infrastructure” with monitoring and reporting of cyber security threats to essential services.