WILMERHALE

Trouble on the Horizon: What ENISA's Report Tells Us About the Threat of Data Breaches

FEBRUARY 7, 2018

Last month, the European Union Agency for Network and Information Security (ENISA) published its 2017 'Threat Landscape Report'[1]. The Report comments on general trends in the area of cybercrime, and identifies and gathers data on 15 top "cyber-threats". Many of the threats identified in the Report are designed to target vulnerable individuals. However, one particularly topical cyber threat draws concern both from individuals and organisations: the increasing threat of large scale data breaches.

The Report's findings in this area make for troubling reading. In the first half of 2017 alone, 2,200 data breaches were reported, exposing over 6 billion records. The largest 10 of these breaches exposed a staggering 5.6 billion of those 6 billion records. Insider threats may be involved in fraud, information theft, or sabotage, and in around 60% of cases, data obtained in these incidents will then be traded for cash.

According to the Report, 35.4% of incidents targeted entities from the medical and healthcare sectors. The government, military and educational sectors also make up a significant portion of reported breaches. However, although the tally of reported incidents is spread across a number of different sectors, the private sector takes by far the largest hit in terms of actual volume of breached data, accounting for 93% of all records exposed. It is not just large businesses being targeted either: 61% of the data breach victims in ENISA's report are businesses with under 1,000 employees.

ENISA makes specific recommendations to assist organisations in protecting themselves against a potential data breach, for example encrypting sensitive data, effective security across all electronic devices, and employee training. The Report acknowledges that for many institutions, the *ex-post facto* legal, financial and reputational consequences of a data breach can be devastating, regardless of the protective measures put in place. It recommends that "*a holistic plan should cover two distinct parts of a data breach incident – assessment of the privacy incident and development of an appropriate breach response*"[2]. While helpful, this advice is vague, and many organisations – particularly smaller organisations with fewer resources – may be left wondering what is needed practically to achieve this.

Looking forward, there is clearly an urgent need for organisations at every level to improve their resilience against cyberattacks, including data breaches. This is particularly the case given the onerous penalties for personal data breaches contained in the General Data Protection Regulation, which will come into force in May this year. However, as the Report points out, this is not at present a fair fight: "*the cybersecurity community is still far from striking the balance between defenders and attackers*"[3]. Cybercriminals are becoming more sophisticated in their methods, and in evading detection. They are monetising their activities in new ways, and benefitting from a rise in the use of opaque digital currencies. Public awareness of issues around cybercrime is increasing, but individuals – and indeed large organisations – lack the skills or infrastructure needed effectively to combat cybercriminals. Improving resilience against cyberattacks may not therefore be enough on its own: organisations should also plan for the worst.

---

[1] ENISA Threat Landscape Report (*ENISA, January 2018*)
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

[2] *Ibid*., p. 74

[3] *Ibid*., p. 7