Organisations overwhelmed by security breaches, as incidents reported to ICO almost double in a year

Submitted by: Huntsman Security
Wednesday, 31 August 2016

Finance Sector Attracts 33% of all Financial Penalties, While Only Responsible for 6% of Incidents.

Data disclosed in error and breaches in security were the primary reasons for an 88% rise in self-reported data protection breaches between 2014-15 and 2015-16 (1), according to a Freedom of Information request by Huntsman Security. 2,048 incidents were reported to the Information Commissioner's Office (ICO) between April 2015 and March 2016, up 88% from 1,089 in a similar period the year before. In fact, there were more incidents where the ICO took 'No Action' in 2015-2016, than were reported in all of the previous year (2).

"Unfortunately, this is not the full story. The average organisation is subject to multiple breaches, of which only some will be detected, so the figures reported to the IOC are likely to be understated," said Peter Woollacott, CEO, Huntsman Security. "The root of the problem is that organisations are under such an intense barrage of cyber activity that threat alerts; many of which turn out to be benign are overwhelming cyber security teams. There is simply too much data to analyse and verify manually. Genuine threats require immediate attention but frequently the investigation of benign and even false alarms can waste a great deal of valuable time and resources. Verizon's DBIR 2016 gave a clear illustration of this problem, revealing that whilst 84% of attacks compromise their targets within days or less, under a quarter are detected within that timeframe."

Interestingly, certain industries are showing especially concerning results (3). For instance, organisations in the financial sector were responsible for reporting less than 6% of all incidents, yet they attracted 33% of all financial penalties pursued by the ICO; suggesting that when finance businesses suffer data breaches, they are of a particularly severe nature.

"Quite simply, no news is bad news: if breaches aren't being detected, it most likely just means that security analysts are having difficulty finding the needles in the haystack. To help them see through the noise generated by security alerts, organisations must find a way to automate threat verification and eliminate the wasted effort that result from false alarms. By using machine learning to identify otherwise "invisible" threats, security analysts can easily identify those that really matter, and as a result, significantly reduce their time at risk from cyber threats. This in conjunction with automation and streamlining the incident management process means that organisations can put themselves, the ICO and the wider public at greater ease that our data is safe in their hands."

The results of the Freedom of Information request also exposed a number of interesting statistics in certain key sectors:

- The sectors responsible for most data breaches remained consistent; with health, local government and education responsible for the majority of data breaches, accounting for 64% of all reported breaches (3).
- UK utilities companies reported only two security breaches to the ICO over the entire 1-year period; but considering that these critical infrastructure companies present a high risk target the numbers demand closer scrutiny.

- Despite a reputation in previous years for poor performance, Local Government shows some signs of improvement compared to many other sectors, with the number of security breaches rising by only 14%. Overall, 70% of all incidents reported by government bodies were due to disclosure of data in error; meaning reducing or identifying possible signs of human error or anomalous activity should be a priority.

FOOTNOTES:

1) Nature of breaches:
   Disclosure 1,369
   Security 623
   Other 56

2) Action taken by ICO:
   No Action 1,544
   Data Controller action required 381
   Improvement Action Plan agreed 50
   Undertaking served 26
   Other 47

3) Breaches by sector:
   Health 941
   Local Government 202
   Education 172
   General Business 134
   Charities 76
   Solicitors / Barristers 72
   Lenders 64
   Policing and criminal records 61
   Housing 51
   Others 275

END

About Huntsman Security

Huntsman Security pioneered intelligent enterprise and cyber security with its landmark platform, Huntsman® Enterprise SIEM, incorporating Behaviour Anomaly Detection (BAD). The Huntsman Analyst Portal™ adds a whole new level of intelligence to automated incident response and the threat resolution process. Huntsman patented key aspects of BAD to detect anomalies in real time and so provides early warning of cyber threats, data leakage, malware and fraud. Huntsman® is a defence-grade cyber security platform which includes threat detection, security analytics and incident resolution. Huntsman is deployed in central government, finance and infrastructure environments in the UK, Japan and Australia. See www.huntsmansecurity.com (http://www.huntsmansecurity.com).

Huntsman Security Media Contact

Dominic Walsh
www.huntsmansecurity.com
+44 (0) 845 222 2010
media@huntsmansecurity.com
@tier3huntsman (http://twitter.com/tier3huntsman)