Most ICO data breach reports late and incomplete prior to GDPR, reveals Redscan FOI request

Submitted by: Redscan
Sunday, 10 March 2019

London, UK, 10 March 2019 – Redscan (https://www.redscan.com), the threat detection and response specialist, today released new Freedom of Information (FOI) request data from the Information Commissioner's Office (ICO). It found that businesses routinely delayed data breach disclosure and failed to provide important details to the ICO in the year prior to the GDPR's enactment.

On average, businesses waited three weeks after discovery to report a breach to the ICO, while the worst offending organisation waited 142 days. The vast majority (91%) of reports to the ICO failed to include important information such as the impact of the breach, recovery process and dates. The FOI also revealed that hackers disproportionately targeted businesses at the weekend, while many reports would be issued to the ICO on a Thursday or Friday – possibly in an attempt to minimise potential media coverage.

Redscan analysed 182 data breach reports triaged by the ICO in the financial year ending April 2018 (relating to 'general businesses' as well as financial services and legal firms)*. Key findings include:

• On average, it took companies 60 days to identify they'd been a victim of a data breach, with one business taking as long as 1320 days
• After identifying a breach, it took businesses an average of 21 days to report it to the ICO, while one took as long as 142 days
• More than 9 out of 10 companies (93%) did not specify the impact of the breach, or did not know the impact at the time it was reported
• Less than a quarter (45 out of 182) of businesses would be compliant with current GDPR requirements, which demand organisations report a breach within 72 hours of discovery
• Nearly half of data breaches were reported to the ICO on a Thursday or Friday (87 of 181)
• Saturday is the most common day for businesses to fall victim to a data breach – over a quarter of incidents were reported on a Saturday
• Financial and legal firms identified and reported breaches more promptly than general businesses

"Data breaches are now an operational reality, but detection and response continue to pose a massive challenge to businesses", said Mark Nicholls, Redscan director of cybersecurity.

"Most companies don't have the skills, technology or procedures in place to detect breaches when they happen, nor report them in sufficient detail to the ICO. This was a problem before the GDPR and is an even bigger problem now that reporting requirements are stricter."

On data breach identification/discovery

Redscan's FOI request reveals that financial services and legal firms were far better at identifying and reporting breaches than general businesses – likely due to increased regulatory awareness and the highly sensitive nature of data processed in these industries. On average, financial services firms took 37 days to identify a breach, legal firms took 25 days, while companies classified as 'general business' took 138 days.

Financial services (16 days) and legal firms (20 days) were also quicker to disclose breaches to the ICO

than general businesses (27 days).

38/181 (21%) organisations did not report a breach incident date to the ICO, suggesting they either lacked awareness of or knowingly withheld this important information. A further 46/181 (25%) organisations also failed to report a breach discovery date.

Mark Nicholls: “The fact that so many businesses failed to provide critical details in their initial reports to the ICO says a lot about their ability to pinpoint when attacks occurred and promptly investigate the impact of compromises.

“Without the appropriate controls and procedures in place, identifying a breach can be like finding a needle in a haystack. Attacks are getting more and more sophisticated and, in many cases, companies don’t even know they’ve been hit.”

“In general, firms operating across the financial and legal sectors are among those better prepared to manage data breaches. The fact that even businesses in these high-value sectors were taking two to three weeks to divulge incidents is a key reason why the reporting rules have since been tightened.”

On the weekend threat / Friday disclosures
Mark Nicholls: “Detecting and responding to breaches is now a 24/7 effort. Many organisations lack the technology and expertise they need, which is compounded by a global cybersecurity skills shortage. Resources are stretched even further at weekends, when many IT teams are off-duty – exactly why hackers chose to target businesses out of hours.

“It’s also interesting to note that nearly half of reports to the ICO were submitted on a Thursday or a Friday, good days to bury bad news. This might be overly cynical but I suspect that in many cases, breach disclosure on these days may have a deliberate tactic to minimise negative publicity.”

The impact of the GDPR
Mark Nicholls: “It’s incredibly optimistic to think that businesses are better at preventing and detecting data breaches since the introduction of the GDPR. Despite the prospect of a larger penalty, many are still struggling to understand and implement the solutions they need to achieve compliance.”

Notes for editors
* Redscan received anonymised data relating to 181 cyber incidents reported to the ICO by finance, legal and general business organisations in the financial year ending April 2018. The ICO had previously published the existence of these incidents on its ‘Action we’ve taken’ site https://ico.org.uk/action-weve-taken/, but Redscan requested additional data supplied in these reports covering:

- The impact on the organisation
- Recovery time
- Number of days between data breach incident and data breach discovery
- Number of days between data breach discovery and disclosure to the ICO

• Day of week when disclosure was made to the ICO

The data was requested on 25th October 2018 and supplied by the ICO on 9th January 2019.
The GDPR came into effect on the 25th May 2018.

About Redscan
Redscan is an award-winning provider of managed security services, specialising in threat detection and integrated response.

Possessing a deep knowledge of offensive security, Redscan's experts are among the most qualified in the industry, working as an extension of clients' in-house resources to expose and address vulnerabilities plus swiftly identify and shut down breaches. Services offered include Managed Detection & Response, CREST-accredited Penetration Testing and Red Team Operations.

By understanding how attackers operate, leveraging cutting-edge threat intelligence, and offering highly acclaimed customer service, Redscan's cyber security professionals can be trusted to provide the insight and support needed to successfully mitigate information security risk and achieve compliance standards.

The choice of industry leaders, Redscan boasts excellent customer satisfaction and retention levels. Security certifications held by the team include: CREST CRT, CCT APP, CCT INF, CC SAS, CISSP, CEH, Security+, CISM, OSCP, SFCP, CCNA, and ISSAP.

Media contacts
Mike Marquiss
Mike@DecodedComms.com
07510 564 704