ROPES & GRAY

ALERT

Privacy & Cybersecurity

July 10, 2018

Thoughts From the London Cybersecurity Breach Response Roundtable

Overview

Attorneys
Rohan Massey

It has been six weeks since the GDPR came into force, and as the consent and sign-up emails slowly stop flooding into our inboxes, the attention has started to shift from GDPR readiness and compliance to GDPR enforcement and breach response readiness.

Under the GDPR, organizations have a mandatory obligation to report a personal data security breach to regulators, and potentially face higher fines of up to €20 million or 4 percent of annual global turnover, whichever is higher, should they fail to implement appropriate security measures to protect personal data.

Ropes & Gray recently hosted a roundtable with FireEye, a cybersecurity and breach response consultancy, and Fleishman Hillard, a public relations firm focused on crisis communication, to discuss actions that should be taken in response to a security incident and what conditions would require a mandatory breach notification to the supervisory authority for a personal data breach. The roundtable provided valuable lessons because of the breadth of attendees, which included those in GC, HR and IT roles from organizations that varied in size and sector, including financial services, private equity, commodities and insurance, and also the fact that the scenarios were interactive, allowing everyone to vote on, and subsequently discuss, what action they would take in each scenario.

Simulated Security Incident

The exercise consisted of 12 scenarios that made up a continuing escalation of a potential cybersecurity incident. These included (i) computers running slowly and crashing; (ii) malware found on a small number of computers; (iii) malware found on an administrator's computer; (iv) an infected computer "beaconing" out to the command or control server of the hackers; (v) login attempts at unusual hours; and (vi) personal data being lost as a result of the security incident.

As the audience ran through each scenario and voted on the suggested course of action, it became clear that there was no consensus on the response. In fact, in none of the scenarios did all the participants agree on the same course of action when responding.

Following each vote the subsequent discussions highlighted how people in different departments or roles within an organization assessed the incident. A good example was the response to the scenario relating to malware being found on a small number of computers. While some attendees thought this was a serious incident, it was those in IT departments who felt that this was a lower level of risk and not a "red flag" issue yet. The IT participants went on to explain that they encounter hundreds, if not thousands, of attempted breaches a day that need to be reviewed in order to decide whether they pose a high enough risk and should be escalated.

Breach Notification

At each stage of the exercise the question was raised as to whether a mandatory breach notification to the supervisory authority would have been triggered. Under the GDPR, a data controller is required to notify the relevant supervisory authority for a "*personal data breach*" within ***72 hours*** of becoming "*aware*" of the breach. So the two biggest

considerations the audience reflected on were: (1) what constitutes a "*personal data breach*"?; and (2) when is the data controller "*aware*" of the breach?

First, the audience broke down the meaning of "*personal data breach*" into two parts:

1. Is the data at issue personal data governed by the GDPR?
2. Has there been the requisite triggering event with respect to that personal data: a (i) breach of security (ii) leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data?

Second, the audience considered the meaning of "*aware*" to be when the data controller has a reasonable degree of certainty that a security incident has occurred and that it has led to personal data being compromised.

As each of the scenarios played out, the audience deliberated as to whether the security incident would require a notification to the supervisory authority for a personal data breach. The outcome was often split as to whether the threshold had been crossed and a notification would be required. While many in the audience recognized that a breach notification would be required if personal data had been unlawfully sent externally, the response was more divided when the scenario involved malware being found on an organization's IT system.

Reputational Considerations

What became apparent throughout the exercise was that reputational damage from a personal data breach was just as much, if not more, of a concern to those in the audience than any regulatory sanction or fine. Many in the audience recognized the importance of an organization being trusted by the public to protect their personal data and the adverse impact that a notification of a security breach can have if not handled correctly.

This issue was particularly relevant during one of the scenarios in which the CEO was considering making a public statement on a personal data breach and was deciding what to say. The subsequent discussions from this scenario highlighted the value of an organization not only having a suitable IT plan in place to respond to the breach but also an effective crisis communications strategy prior to making any public announcement.

Next Steps

The lack of consensus from the audience highlighted that the best form of preparation for a security incident is to ensure that there are clearly defined policies and procedures in place to provide a coordinated and appropriate response from all business lines, for instance: (i) identifying stakeholders responsible for managing security incidents; (ii) the internal decision-making flow chart; (iii) the escalation process and timetable (for both internal and external actions); (iv) the process for categorizing the risk of the security incident; and (v) the obligations to record and document each step and the rationale for response when dealing with the security incident.

If (and most likely, when) a personal data breach occurs, having these policies in place can assist in coordinating the response. This response may differ depending on an organization's size, structure, attitude to risk and/or industry sector, but failure to implement and enforce these policies increases the risk of an organization incurring a higher fine from the supervisory authority, as well as the negative PR and reputational consequences that come with it.

Finally, it became clear as the roundtable progressed that informing the legal team, PR team and external incident response providers early on, and having them on call and ready to act immediately, were vital in an organization's preparation and response to a security incident. It is much easier to scale down a response than scale up and such preparation will therefore place an organization in a much stronger position should they suffer a personal data breach.