Burn, baby, burn

Ford Kuga, Samsung, reputation management and POPI

During January 2017 Samsung announced the results of a months-long investigation when some of the devices it was selling started to self-ignite. This saw a steep decline in its global reputation, resulting in a recall of 2 500 000 Galaxy Note 7 units.

This was not the first time a tech device has experienced such problems: do you remember the issues Dell (at one time the world's largest supplier of PCs) had in 2006 when some of its laptop batteries also displayed auto-combustion characteristics and it recalled 4 000 000 of them?

Of course you can see where this story line leads us already – the Ford Kuga debacle which has been almost constantly in the media over the last few months, with a much more modest recall target of only 4 500 Kuga units.

When your good name is on the line, and you enjoy global recognition for your brand, the value of effective reputation management is kind of obvious. So what has this got to do with the POPI Act? A great deal, if international experience is anything to go by.

When the Information Regulator announces commencement of the 12-month transition period to full effect of the POPI Act (which had not happened at the time of writing this article, but is widely expected in the first half of 2017), there will be a number of possible negative consequences to non-compliance with the Act. Whilst a security compromise (more often called a data breach in global markets) is the most obvious concern, there are numerous other grounds on which the Regulator and interested stakeholders (data subjects to use POPI parlance) may feel they have reason to take action where failure to comply with the Act is concerned. Any and all of these possible failures could have the direct negative consequences of a monetary penalty (issued by the Regulator), civil damages claims (from data subjects) and the costs of disruption to normal business in the recovery period after an incident has occurred, potentially including revenue lost from disaffected current and future clients.

Not yet mentioned in this article but almost certainly surpassing all the other negative impacts to be expected, but not welcomed, is reputation damage. That's where the Kuga and POPI non-compliance have something in common: headlines for all the wrong reasons. International surveys conducted over the last few years by information security companies such as Kaspersky Lab and Trend Micro provide some indication of the types of risks that need to be addressed where personal information protection is concerned.

So what action is recommended to help to manage your reputation when it comes to POPI? Clients of mine have evaluated several frameworks which can be used to better manage their compliance activities. One of the most popular is from the US which is part of the Obama legacy from 2014 (not yet overturned by a Trump Executive Order at time of writing) that offers the following five groups of the Cybersecurity Framework Core Outcomes which can help with protecting your reputation, whether you are in Bloemfontein, Benoni or Bloubergstrand:

- **Identify** – develop the organisational understanding to manage cybersecurity risk to systems, assets, data and capabilities.
- **Protect** – develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect** – develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond** – develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover** – develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

If you follow this advice your reputation is less likely to get burned than Samsung, Dell or Ford. Good luck with managing your reputation. ■

Cost of security incidents by type (high to low)

- Failure of third party suppliers
- Fraud by employees
- Cyber espionage
- Network intrusion/hacking
- Intentional leaking
- Phishing
- Accidental leaking
- Malware/viruses
- DoS/DDoS
- Software vulnerabilities

Top three major consequences of a breach:

- Loss of access to business-critical information
- Damage to company reputation
- Temporary loss of ability to trade

Top three most expensive types of security breaches:

- Third-party failure
- Fraud by employees
- Cyber espionage

Top three IT security threats that lead to data loss:

- Malware
- Phishing attacks
- Accidental data leaks by staff

Source: Kaspersky Lab report: Damage Control: The cost of Security Breaches

ACKNOWLEDGEMENT
PETER TOBIN