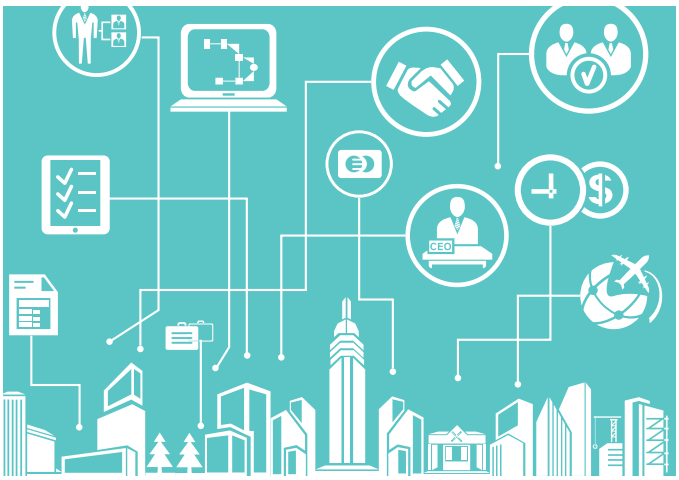
The Economist Intelligence Unit

TOO MUCH INFORMATION

Social media risks go beyond reputational damage

Written by The Economist Intelligence Unit



Before Lewis Hamilton made a high-profile switch to a rival team, the Formula 1 driver was publicly chastised by his McLaren teammates for sharing a photo of his qualifying telemetry data with nearly 2m Twitter followers. It was a classic careless information leak, directly to the competition. "The mistake that Lewis made", McLaren's technical director said at the time, "is that he didn't appreciate the nature of that information. We spend our lives trying to keep things like that secret."

Mr Hamilton's error was high profile, but not unusual. Employees have a propensity to underestimate the value of information they have access to. They also underestimate the risks of sharing this information. "In social media there's a blurring between social and work life," says Mark Elliot, an academic specialising in privacy and disclosure at Manchester University. "If your life-story narrative crosses the work-life boundary, as everybody's does, it's difficult not to reveal information about what's going on in your workplace on social media. The degree and scope of this is very difficult to estimate."

According to senior executives surveyed by The Economist Intelligence Unit, employee carelessness is considered the main source of risk to their organisation's information, above hacking or technology failure. The rise of social media in recent years simply means that each employee is capable of leaking proprietary, confidential or market-sensitive information at a thumb tap, causing financial and competitive loss, reputational damage or any number of legal headaches.

This may damage the company, or it may damage the employee; often, it can do both: in 2010 a contract worker was fired from a Michigan hospital for posting negative comments about patients on Facebook, violating confidentiality rules. It is hard to imagine that nurses were not complaining about patients after hours before Facebook, but as communication is now more public the problem is magnified—and has become a public relations issue, too.

With higher profiles and greater exposure to sensitive information, together with a relatively weak grasp of social media, senior executives are a reliable source of risk. Last year the CFO of a US women's retailer tweeted about company financials before the company officially announced its earnings, sending the share price soaring. The CFO was subsequently let go for improper social media use.

Like the hospital worker, the ex-CFO violated well-established rules—in this case the fair-disclosure regulations of the US Securities and Exchange Commission (SEC) over how listed companies publish information. Indeed, this particular breed of social media faux pas involving executives of listed companies is not uncommon; a few months later the CEO of a US online media company attracted the SEC's attention after sharing material information on his personal Facebook page. The SEC may have loosened the rules earlier this year, making such use of social networks acceptable under certain circumstances, but a change in regulation does little to change the underlying conduct of employees.

LINKED IN-FORMATION

The aforementioned individuals should perhaps have known better, but future risks are likely to be more subtle—and more dangerous. Seemingly innocuous information may provide insights unknown to the discloser when patched together with other sources. For a sense of what can be done, consider Netflix.

In an exercise in crowdsourcing, the company shared its vast repository of users' movie-watching data, to encourage third parties to improve on its recommendation algorithm. The hope was that others would spot patterns in users' viewing history that might help to predict what new films users might like to watch next. The data was nominally anonymised by scrubbing associated personal information and providing only lists of movies watched by a given user ID.

Proving a point, university researchers managed to match the anonymous viewing records of individuals on Netflix with profiles elsewhere online; for instance, profiles on websites like IMDb, a movie

community[1] . These overlaps revealed identities of some Netflix users, including their full viewing history. One, a lesbian not open about her sexual orientation, sued Netflix for publishing revealing information this way[2]. The company settled.

Employees may be sharing seemingly innocuous information of this kind entirely unawares, exposing companies to significant—and unknown—information risk. Here ignorance is a greater threat than carelessness. "It's quite extraordinary how much information we see leaked through an individual's LinkedIn page," says Alastair Paterson, CEO of Digital Shadows, a cyber-security firm.

A typical employee giveaway is the software versions that a company runs internally. This can allow attackers to exploit vulnerabilities in that software. "In isolation, one profile may not yield much information, but in aggregate across an entire organisation it is possible to build up a detailed picture of how their technology platform operates and who their key individuals are, opening them up to attack," says Mr Paterson.

Amar Singh, the chief information security officer of a FTSE 100 company (which requested not to be named), believes that the modern tendency towards "oversharing" of data through mobile devices and social media should be at the forefront of managing information risk at most organisations. In his view, there are two methods of protecting the information most critical to the company: one is technology; the other is people. Whereas technology continues to advance, making incremental improvements to security and protection, humans remain the weakest link.

"Until we all turn into cyborgs we will need to employ humans to plan, build, configure and maintain our digital systems and the data in those systems," says Mr Singh. "These users are intentionally or accidentally sharing mostly useless information via their smart devices, but sometimes it can be very useful and critical information, which often forms the basis of some of the most complicated attacks."

PATCHWORK

As the risks surrounding social media are mostly related to conduct, they could—in some respects—be easily solved. Much can be achieved by simply raising awareness, both of the value of information and of the risk of disclosure. "Focusing on the technology used for communication will not work," says Andrew Walls, a research vice-president at Gartner, a consultancy. Mr Walls suggests a thoughtful social media policy should begin with education, and include clear mandates about content, timing, best practices and workflows.

This extends beyond "be careful what you tweet", to formalising guidelines about communications practice more broadly and addressing the difficulties of keeping a record of all this unstructured information. The real difficulty comes with putting these guidelines into practice, particularly when companies continue to underestimate the scale of the risk. "Most senior executives I speak with are aware of the basic nature of these risks but are not able to reliably estimate the probability of occurrence," says Mr Walls. Judging by the actions of the senior executives above, giving social media training to the C-suite would be a good place to start.

[1] www.securityfocus.com/news/11497

[2] www.wired.com/threatlevel/2009/12/netflix-privacy-lawsuit/