

Where to find unusual inspiration for protecting business secrets

Knowledge is power

Whether in politics, in battle or in business, usually the upper hand is with the party that is better informed and/or is better able to analyze the data they have. Thinking about this I wondered whether this is symmetrical. In other words, whether a loss of data also automatically equates to a loss of power. Sometimes it does. When the USA in the late 1940s discovered that the USSR had stolen its atomic weapon secrets, this suddenly redefined the global power equation. And obviously not in the US' advantage. What is true in the military similarly applies in business. Business secrets are also worth protecting. They need protection against ordinary humans; people like you and me. As I will show below the biggest risk of losing secrets relates to the human tendency to spill them.

People need help to keep secrets

The British during their long history as a maritime power traditionally vested their trust in their naval superiority. The English coined the telling warning "loose lips, sink ships" to prevent the English population during World War Two to spill secrets. Secrets were, however, not only lost to the West of the English Channel. The German war effort also had its share of issues with the loss of secrets.

Former German intelligence officer Walter Schellenberg in his memoirs vividly describes how a Yugoslavian human intelligence collector effectively gathered critically relevant German military data in Berlin in 1941¹. The Yugoslav simply appeared at the right dinner parties with the right high-society people at the right time. Schellenberg rants that the Yugoslav did not even have to spend out-of-pocket money, whilst the loose talk he collected indeed did put German lives at risk:

"The amount of highly secret and vitally important information that was bandied about in these circles was really incredible; and so, too, was the extensive harm such careless and stupid gossip could do. The guilty ones were all highly intelligent people, leading engineers, architects, officials and officers of the German Reich"

Even when he wrote his memoirs in prison almost a decade later, Schellenberg's anger is still tangible. Connecting the dots, the Yugoslav could forewarn his Government of an upcoming air raid on Belgrade; the first of its kind and one meant to come as a surprise. Just to keep the perspective right: this happened at the time that Germany fought an all-out war. When even in times of war people cannot resist the urge to share secrets, what will happen in business in peacetime?

Most people love to talk about their work – trading secrets for recognition

Business research published in 2010 does not suggest that human evolution in the period 1940-2010 has made people more apt to keeping secrets². When describing how businesses can improve their processes by improving *knowledge brokering* the researchers observe:

“Most experts, we find, happily share their experiences free of charge since they too benefit from the interactions [of knowledge brokering]. Further, we find that most managers simply enjoy the experience of sharing their stories and helping to develop new approaches. Suppliers, an ideal source of brokering opportunities, are typically delighted to help”

In short: people enjoy telling what they know. Whatever the motive; be it helpfulness or recognition, secrets may get spilled by humans satisfying other needs. When enjoyment, recognition or convenience butts’ heads with confidentiality, guess who wins³?

A relatively recent and extremely dangerous medium for the loose talk of today are social media. Examples are known of executives polishing up their publicly available résumés through sharing trade secrets like the sales figure they are responsible for or the number of staff they manage in sales in their channel or geo-territory. Highly secret innovations occasionally appear first in the public domain in careless postings as personal achievements.

Business leadership needs to set the example before starting trainings

A company that aims to keep its secrets needs to protect them. This includes installing effective cybersecurity technology and ensuring there is a physical barrier against intruders. Most important, however, remains the human factor. There is indirect evidence that corporate friendliness significantly reduces your risk of losing trade secrets due to unhappy company staff intentionally divulging them⁴.

Even the friendliest of companies, however, needs to train its staff in trade secrets protection. It starts with management. They must set an excellent example. When all staff see the credible and uncompromising compliance of management to the own rules, management may usefully start communicating the “clear message that [information] security is everybody’s job”⁵.

If one country has historically set the example in trade secret protection it was Japan. Even in an overseas plant of Fuji Film in Europe a supplier could in the past only enter the production hall where one of its supplied machines required maintenance when all production had stopped *and* when all neighboring other machines had been covered with non-transparent plastic foil. A visit to the hall revealed nothing but what the visitor had to see. This approach seems deeply embedded in Japanese culture. A Japanese saying that anyone passionate for trade secret protection should know goes like this⁶...

“Behold the frog who when he opens his mouth displays his whole inside”

Notes:

- .1. Schellenberg, W. [2000], *The labyrinth, memoirs of Walter Schellenberg, Hitler's Chief of Counterintelligence*, Da Capo Press, Cambridge, Massachusetts, pp. 175-183.
- .2. Billington, C., Davidson, R. [2010], Using knowledge brokering to improve business processes, McKinsey Quarterly, January 2010.
- .3. Brenner, J.F. [2007], Counterintelligence in the 21st century, not just a Government problem, paper delivered at the AFCEA Counterintelligence Conference, Sunnyvale CA, Dec. 4, 2007, p. 4.
- .4. The evidence I have points at the effectiveness of friendly intelligence collectors targeting unhappy company or military staff (see: Grey, S. [2015], *The new spymasters*, Penguin, London). My statement is: what if a company is friendly – that would give 'friendly foe's collectors' little chance.
- .5. Palmquist, M. [2014], The security risk in the cubicle next door, Strategy & Business blog, Nov. 6.
- .6. Benedict, R. [1954], *The Chrysanthemum and the Sword; patterns of Japanese culture*, Tuttle Publishing, Tokyo / Periplus Edition reprint, p. 216.