

How to protect secrets through studying the psychology of defectors

Secrets are spilled all around us

Revelation upon revelation hits the press. Leaks have always been there, but in today's post-truth world the frequency of leaking looks to hit all-time-high levels. Clearly, Wikileaks with its enigmatic leader Julian Assange has already been around for some time. Edward Snowden's spilling of NSA-secrets is already old news, even when his self-serving biography sells like crazy. Thinking about this, some questions came to my mind:

- what is a secret?
- what is the purpose of spilling secrets that makes spilling so popular?
- who are those that are inclined to spill secrets and why do they do it?

Below I will address the first two questions superficially. The third question gets the focus of this article. The answer to the third question may contribute to protecting your secrets and that of your business from those that may now or tomorrow not be able to hold those secrets. So: what is a secret?

Secrets are meant to hide truths that hurt when they are revealed

A secret may be simply defined as a (set of) data point(s) that a party tries to keep other parties from knowing. The data point may range from the most sophisticated software algorithm to encrypt wireless communication to the simple fact that you stole an apple. In both cases, the data point is kept secret to prevent loss. In the case of the algorithm, encryption by definition ends when everybody can know your encryption key. In the case of the apple, the secret is aimed to protect you from the punishment that may inevitably follow upon the crime being revealed. You do not need to be an ardent reader of Dostoyevsky to know that the revealing often makes the crime.

The above consideration may also bring us closer to why revealing other party's secrets currently seems so popular. Losing a secret by definition hurts the holder of the secret. In today's polarized and unstable political climate, interests vary widely between different individuals and parties. The hunting for and the leaking of the other party's secrets in the currently revitalized cold war thus seems to have a similar purpose today of what mutual artillery barrages a century ago had in trench warfare. Today we shoot to destroy reputations, because we know the other party equally harshly does the same. In the Great War we fired grenades, today we disseminate the other party's secrets. Today is a bit less bloody perhaps, but probably just as mean. Moreover, when both parties do it, it may be just as endless and futile as trench warfare was in Flanders' fields. The current unfortunate global trend of a gradual loss of freedom-of-the-press seems to point in the same direction¹. The press is perceived as an increasingly unwelcome challenger to the secrets of power, wherever they may be.

This brings me to an interim conclusion: people, especially those in power or in crime - which may not be mutually exclusive - perceive secrets as painful to lose. Making the other party lose its secrets is apparently a form of 21st century (information) warfare. In this way we may stick to the tried-and-tested definition of Karl von Clausewitz on warfare²: making others lose secrets is an instrument of warfare: the continuation of politics with other means. To stick to our metaphor, we may rephrase our third question into: what soldiers do we see in this war?

A paradox: leaks are often inside-out, not outside-in

At this stage we need to make a critical split in our thinking. Secrets may in principle be lost in two ways: inside-out or outside-in. I would define outside-in as a party that sends a collector to illegally obtain another party's secret. Think of the Republican White House under President Nixon sending the 'plumbers' to collect secrets at the Democrat party's Watergate office. This activity is commonly referred to as espionage, with the collector being usually referred to as spy. Once a spy has obtained an adversary's secret, the secret may be revealed or used against the adversary when it hurts most. Spies, however, rarely act alone. Spies need helpers. These helpers may simply provide spies with secrets, e.g. in exchange for cash. Such helpers we normally call traitors. When a traitor entirely switches sides, we tend to call them defector. In some cases, a defector switches sides without any preliminary incentive having been provided or without any prior prompting by a spyhandler³. When a defector after switching sides reveals secrets to the party he or she now feels connected to, I would call it an inside-out loss of secrets.

When studying the world's history, there are plenty of stories about how spies stole secrets. In reality, however, it seems that a lot of spying generates a low yield, unless a helper has pro-actively presented himself or herself, either sticking in his position with access to secrets that he offers regularly or in a one-off defection whilst carrying the secrets. Someone inside your organization that is already helping an adversary but formally is still on your pay-roll is like a chameleon. Inside your organization the person takes the color of your firm, pretending to be one of you. The person's true colors, however, are different. They belong to another firm or another political system or country. Sometimes traitors and defectors get so tied up in their own devious schemes that they no longer know where they or their heart (or what is left of it) really belongs: they simply, like a chameleon, adapt their colors to wherever they are.

As so often, the truths about chameleons from military history also apply in business. Traitors and defectors together cause the majority of business trade secret losses. In spite of all cybercrime, almost 60% of information security professionals pinpoint in a 2014 survey to current or former employees as the most likely source of accidental or intentional leaks⁴.

The question now is not what motivates spies. No matter how we ethically view their profession, they serve their own side, being prepared to do dirty work in the interest of their side. Thus, spies are not interesting. What is interesting is why traitors and defectors do switch sides. What are their drivers to do so? These two questions ladder up to the secrets keeper's ultimate benefit: how can we prevent our own people to betray or defect us?

The answer to the last question is also where the link to my business and work experience comes in. When in a business setting, we love our trade secrets, how can we prevent our colleagues (and ourselves!) to feel the urge to leak them?

We have now seen the relevance of leaks in the 21st century information warfare and relatedly the number of spies around to happily receive secrets from inside-out sources. As a way to discover protection measures, I decided to revisit 1980s cold war studies on the psychology of defectors to find insights on this that are neither new nor secret. Here's what I found.

Money, revenge or shame generally drive defectors

Defectors in business and in the military tend to have one of three motives for leaking (trade) secrets^{4,5}:

- money: the knowledge that (trade) secrets can be sold to an adversary
- revenge: the knowledge that leaking (trade) secrets hurts their former employer: as a way to pay back for some kind of perceived slight
- shame: they offer secrets to prevent the adversary to leak compromising information on the defector

In military intelligence, the acronym MICE is used to characterize motives of defectors: Money, Ideology (= in business: revenge), Compromise and Ego (which may drive a desire for money).

Most defectors move pro-actively. They tend to be driven by either money or revenge. Staff that have been compromised and in return after being coerced start to leak secrets tend to be more common in the military than in business. In a military or diplomatic context, such defectors are often the victims of honey-traps: sexual escapades which have been recorded etc. The use of compromising materials to coerce individuals to leak secrets is also out of scope here. Revenge-driven defectors are the most committed ones to hurt their (former) employers but they are not so common in business. Still, people that perceive to have been done wrong, can upon leaving their employer take a lot of trade secrets with them... Money, however, is the most common driver.

In the 1580s, the Anglican intelligence officer William Parry who served Queen Elizabeth I defected to England's Catholic enemy: The Holy See. His motives were debt (so the need for money), his desire to impress powerful men and as he saw it⁶ "*the bitterness of service left unrewarded*". In the case of Parry, we see three common motives in a single case: money, revenge and recognition. Times change but human nature does not.

In the late 1980s the CIA ran a project called Slammer^{7,8}. This project aimed to understand motives of defectors. In the context of this project, 30 spies that had been convicted and were at the time of the research in prison have been interviewed. Even though over 25 years old this now declassified piece of research provides findings that may still apply to (would be) business defectors today.

Project Slammer reveals money-driven defectors to be calculating the risk/reward balance. They conclude that the money is good and the risk is negligible⁸:

"Most convicts said stealing secrets was so easy that they were motivated to gather classified documents outside their normal areas of access. [...] I was putting my nose in books where I didn't belong... talking to people, gathering information from conversations. It was actually obvious, I felt. Somebody should have noticed [...but] a lot of people just tend to mind their own business."

Intelligence agencies or unethical corporate information collectors of course have not failed to notice the human vulnerability when it comes to obtaining 'easy money'. The Czechoslovakian Government in the 1930s even set up a small bank ran by the military intelligence department, just to seduce cash-strapped Nazi-German citizens with attractive loans. Once the loans had been provided, interests payment terms could include the offering of relevant military secrets instead of cash⁹. Along the same lines, the KGB listed the following preferred attributes of potential British defectors. Again, a disproportional need for money is being highlighted⁵:

“A good agent [from KGB’s perspective, from a Western perspective: a defector] is one whose vital statistics are the following: he works, for example, in a military department and holds a middle-ranking but key position giving him access to information; he doesn’t aspire to a higher office, has a chip on his shoulder about being a failure [...], he drinks (an expensive habit); he has a weakness for the fair sex (which is also not cheap); he is critical of his own government and loyal to the resident’s [i.e. the KGB-chief in Britain] government”.

The above quote on middle managers and on the perception of failure of the defector is also corroborated by 16th century evidence provided below¹⁰:

“the best spies were often humble men. A servant, perhaps unseen and certainly often unacknowledged by his betters, was able to hear and see things other men could not.”

Now, in the upper quote read instead of “own government” the words “own company” and replace “resident’s government” by “the agent that pays him”. After all, to money-driven defectors, ideology is less relevant.

Defectors’ career prospects tend to be modest at best

The quote above still applies to today’s business world. What colleagues are most vulnerable to considering selling your firm’s trade secrets for money? Using the quote, the attributes seem to include:

- **middle-management**, with wide access to information but without strong career prospects, possibly having been (in their own eyes) by-passed for a more senior position they believed they qualified for.
- either aiming to keep up with the Joneses, e.g. their colleagues that are on faster career tracks, or simply having a Bohemian taste, he may **spend more than he can afford**, ending up in debt.

Risk factors for pro-active, money-driven defectors thus include financial stress and an excessive need for approval or recognition, which translates itself in a desire to live above their normal means. Too often, money-driven defectors like Aldrich Ames were caught because they couldn’t explain their luxurious life style, not because they were caught in the act of illegally collecting and disseminating secrets to third parties.

Defectors tend to have common characteristics and attributes

Project Slammer describes how a defector sees himself at the time he starts selling (trade) secrets⁷. He believes...

- *he is special, even unique.*
- *he is deserving.*
- *his situation is not satisfactory.*
- *he has no other (easier) option [than selling secrets to correct his situation].*
- *he is only doing what others frequently do.*
- *he is not a bad person.*
- *his performance in his government job (if presently employed) is separate from espionage; espionage does not (really) discount his contribution in the workplace.*
- *security procedures do not (really) apply to him.*
- *security programs (e.g. briefings) have no meaning for him, unless they connect with something with which he can personally identify.*

He feels isolated from the consequences of his actions...

- *he sees his situation in a context in which he faces continually narrowing options, until espionage seems reasonable.*
- *he sees espionage as a 'victimless' crime.*
- *once he considers espionage, he figures out how he might do it. These are mutually reinforcing, often simultaneous events.*
- *espionage subjects don't see themselves as traitors. Their acts are usually sustained with some measure of comfort and self-justification.*
- *he finds that it is easy to go around security safeguards (he is able to solve that problem). He belittles the security system, feeling that if the information was really important, espionage would be hard to do (the information would really be better protected). This "ease of accomplishment" further reinforces his resolve.*

Project Slammer also describes common attributes of defectors – some of which showed sociopath characteristics. (Would be) defectors may show the following characteristics:

- Easily despairing over their situation
 - Short attention span
 - Polarized relationships/responses
 - Poor relationships
 - Lack of maturity
 - Poor impulse control
 - Sociopathic tendencies
 - Conceited / self-absorbed
- I'm bored
 - With me or against me
 - I'm lonely / alone
 - I want it now
 - Who cares about me?
 - Me, me, me!

(Would be) defectors tend to be:

- unusually calm and stable under stress but cannot tolerate routine or boredom.
- above-average intelligent.
- good verbalizers – sometimes in two or more languages.
- poorly capable to form lasting and adult emotional relationships because their attitude towards others is exploitative.
- skeptical and cynical about the motives of others.
- secretive, enjoying secrecy and deception for its own sake.

The key lesson for business: a happy staff is a joy forever

Defectors as we saw above may either be opportunistic and money-driven or may be acting out of hatred. What all defectors, however, have in common is that they are unhappy about their current situation. The first, rather obvious lesson for business is that to prevent trade secrets to leak, maintaining a happy staff is the best guarantee. It is, however, a dream to expect all staff to be happy all the time. Even when staff are generally properly treated it is not impossible that a staff member starts to feel unhappy - e.g. as a result of financial stress – and may consider to start selling trade secrets.

The trick and first step in a socially healthy business environment is to pick up the early warning signals of this awakening. This is especially true when it is a staff member with a high confidentiality clearance. Combine those signals with the common characteristics as discussed above of defectors, i.e. people that developed into chameleons. This may provide a proper first risk assessment.

Obvious as it may seem, but a second step is to pay attention to the particular individual staff member. Mostly would-be defectors simply need recognition to keep their urge to become a chameleon in check. Recognition is a powerful driver. The expensive watch or car that is to be paid by stealing and selling trade secrets should be noticed by someone after all: recognition is the ultimate driver. It is the unmet need for glory that apparently justified the risk of the very act of stealing.

A would-be defector that has colleagues that treat him or her with kindness and understanding in his or her perceived trying circumstances, may either help them feel remorse about what they may already have done wrong or may help them prevent doing wrong in the first place. Most defectors are too smart to leave traces. Traditional security systems will not easily catch them. Kindness may, however, be the best measure, preventing wrong before it is being done.

Notes

- .1. <https://rsf.org/en/ranking> visited May 2, 2017
- .2. Clausewitz, K. von [1980] (based on edition of 1832-1834), *Vom Kriege*, Philip Reclam, Stuttgart.
- .3. Hoffman, D.E. [2015], *The billion-dollar spy – a true story of cold war espionage and betrayal*, Doubleday, New York.
- .4. Palmquist, M. [2014], *The security risk in the cubicle next door*, Strategy & Business blog, Nov. 6.
- .5. Andrew, C., Mitrokhin, V. [2001] *The Sword and the Shield*, Basic Books (paperback), New York, p. 410.
- .6. Alford, S. [2013], *The Watchers – a secret history of the Reign of Elizabeth I*, Penguin, London, UK, pp. 142, 180 and 190.
- .7. ICS [1990], *Intelligence Community Staff of the Director of Central Intelligence (CIA), memo ICS 0858-90, Project Slammer Interim Report, April 12*, see: http://www.foia.cia.gov/sites/default/files/document_conversions/89801/DOC_0000218679.pdf visited March 14, 2015.
- .8. *Stein, J. [1994], The mole's manual, New York Times, July 5 issue.*
- .9. Moravec, F. [1975], *Master of spies – the memoirs of General Frantisek Moravec*, The Bodley Head Ltd., London, UK, pp. 55-56.
- .10. Alford, S. [2013], *ibid*, p. 75.