**When bubbles burst: Mimetic insights into minimising confidentiality breaches**

**Abstract**

This paper presents a theoretical model to help managers visualize and manage confidential situations more effectively. The model metaphorically likens a confidential setting to the properties of a soap bubble, *eg*. elastic expansion or contraction, minimal surface area to contain a given volume, fragility, surface tension, pressure, stress, strain and the potential for bursting thereby releasing the contents to the external environment. We explore the conceptual developments in two phases. Firstly, looking at how a bubble and confidential scenario form and grow. Secondly, we consider how a bubble may burst and map these forces to ways in which confidentiality may be breached. Many attributes are mapped, the key ones being: the embedded *value* within the system, the *criticality* of maintaining confidentiality, increasing *pressure*, the corresponding *stress*/*strain* dynamics and the levels of *trust* between stakeholders. Key research propositions are derived from the model which aims to minimise the risk of a confidentiality breach.

Keywords: Confidentiality, secrets, communication, whistle-blowing, non-disclosure, trust, metaphor.

**1. Introduction**

Effective communication is central to an organisation’s success; although in commercially sensitive areas a measure of effectiveness can actually mean *restricting* some information flows. At an individual level, entrustment with keeping a secret can be a potential burden as well as a privilege, and a breach of confidentiality can have significant impacts on all stakeholders. Many organizations have blanket disclaimers on communications (especially email) and individuals involved in sensitive arenas are often required to sign a non-disclosure agreement. Despite these ‘legalistic remedies’ (Sitkin and Roth, 1993), the number of information leaks are rising year on year resulting in significant financial and reputational costs (Pouillot, 2011). Some leaks have global consequences as seen on WikiLeaks as well as significant national security breaches as shown recently by the Edward Snowden case. These leaks have the potential to change the geo-political landscape and strain international relations. At the organisational level, many breaches go unreported, although a growing number are making the headlines. A recent report suggests that over $300 billion worth of intellectual property is stolen annually from American organisations (Blair et al., 2013), with cyber-enabled theft emanating from China being a particular issue (Donilon, 2013). The UK’s Information Commissioner’s Office (http://www.ico.org.uk/news/latest\_news) shows a catalogue of fines being levied on organisations for breaches of data privacy, with many examples of significant breaches occurring within the National Health Service. At the individual level, for example, a Credit Suisse executive was recently fine £210k for leaking confidential information prior to a bond sale (Masters, 2012). Despite the increased awareness and regulation of confidential information though, it seems that “…most firms take a primarily reactive approach to managing privacy by waiting for an external threat before crafting cohesive policies that confront their information practices” (Milberg et al., 2000, p.35). It is clear from these examples that there is a significant need to improve our understanding of confidentiality breaches and to develop new theoretical insights into the area. The aim of the present article is to provide managers with a new conceptual model based on the key attributes at play in a confidential setting and how they might interact to give rise to a breach. Such a model should enable managers to manage confidential situations in a more proactive and effective manner.

Cain (1998, p.158) identifies two obligatory conditions of confidentiality: firstly that “information is entrusted by one person to another; and [secondly] there is express understanding that this will not be divulged”. The majority of literature on confidentiality is within the legal and medical domains, with a focus on individual rights and the ethical constraints of disclosure. In the medical arena, part of The Oath of Hippocrates (later written into the Declaration of Geneva) forms the basis for confidentiality expectations of all healthcare professionals, stating that: “I will respect the secrets that are confided in me, even after the patient has died” (WMA, 2009, p.18). The concept of ‘legal professional privilege’ also strictly protects any disclosures that a client might make to a member of the legal profession. By comparison, confidentiality expectations in the management profession are often implicit. This is reflected by a sparse management academic literature in this area which focuses mainly on the ethics of ‘whistle-blowing’ or probabilistic models of breaching confidentiality.

Steele (1989) proposes two theoretical models of expected time until disclosure of a secret. The first, ‘clique communication model’ (CCM), includes the number of people aware of the secret, the rate of communication between any pair of individuals who are in on the secret and the probability of compromise in confidentiality. With CCM, the “expected window of secrecy decays quadratically with the number of people who are in on the secret” (Steele, p. 242). Expanding on the CCM, the ‘birth process model’ (BPM) “acknowledges that simply enlarging the pool of people who know the secret does not automatically constitute disclosure” (Steele, p. 243). Instead, BPM focuses on “when the secret is eventually communicated to a *leaker*, *ie*. a person who leaks the secret immediately after learning it” (Steele, p. 243). The effects of such information leakage have also been modelled in a supply chain context (Anand and Goyal, 2009; Li, 2002; Li and Zhang, 2008). Other models of confidentiality exist, although they are mainly linked to cyber-security within electronic systems (*eg*. Rukšėnas, 2008; Shing et al., 2009). Underlying these models are the behavioural aspects of disclosure, especially the role of trust (Harwood and Ashleigh, 2005) and codes of ethics (Gaumnitz and Lere, 2002). Phillips et al. (2009) also explore the role of status distance associated with demographic characteristics and how this impacts on the willingness of individuals to disclose personal information to others. Majchrzak and Jarvenpaa (2004) combine many of these aspects in their conceptual framework of ‘organizational levers’ to help balance the individual factors that might give rise to a breach of confidence.

As explained earlier, most of the wider literature on confidentiality comes from the legal and healthcare sectors which primarily discusses the ethical ‘rights or wrongs’ of disclosure (Gewirth, 2001; Hook and Cleveland, 1999; Rae et al., 2002; Smith, 2000), rather than explore the underlying processes of a breach. Of the literature that specifically covers the breach mechanisms, emphasis is placed on developing probabilistic models containing just a few variables; but these do not approach the issue in any holistic sense by combining quantifiable attributes with their underlying behavioural aspects. Some existing models are also limited in their visual or conceptual clarity, making then potentially difficult for managers to use in a practical sense. These limitations, together with the increasing number and scale of leaks within organisations, provide the need for a new approach to understanding the mechanisms behind a breach in confidentiality.

In previous work, Harwood (2006) outlines broad conceptual similarities between the characteristics of confidentiality and a soap bubble. The principal simile is the need for confidentiality constraints to constantly retain their ‘stretch’, thereby expanding or contracting to accommodate an optimum volume with a minimal surface area at any given time (to minimize the exposure to ‘outsiders’). Other similarities relate to the fragility of bubbles and confidentiality agreements, where the bubble may burst with the information dissipating into the environment. The scientific processes behind a natural bubble’s lifecycle (inception, growth, maturity and ultimately demise) have been explored in some depth (Feng and Leal, 1997; Plesset and Prosperetti, 1977; Reissner, 1956). By building on Harwood’s (2006) work, we now take the main physical processes at play in a bubble and conceptually map them across to the management of confidential information, with a specific focus on maintaining the bubble’s integrity. In doing so, we tackle the limitations of existing approaches by developing a more grounded theoretical ‘frame’ or model, one in which combines multiple attributes, sets confidentiality in a dynamic system and is intuitively accessible to help managers actively minimize the risk of a confidentiality breach.

**2. Gaining insights through metaphor**

The role of metaphor in the production of knowledge can be traced to Aristotle’s *Rhetoric*; and many of the significant theoretical advancements in social theory since have been explained through metaphor (Morgan, 1997; Ortony, 1993). Glucksberg (2003, p. 92) describes the use of metaphor in ordinary conversations, and that “we understand metaphorical meanings as quickly and automatically as we understand literal meanings”. Metaphor has been used to explain phenomena across a range of business-related topics, such as: organizational change (Cornelissen et al., 2011; Waistell, 2006), purchasing and supply management (Ramsay and Croom, 2008), organizational values (Waistell, 2007), marketing (Capelli and Jolibert, 2009), organization theory (Cornelissen and Kafouros, 2008) and operational research (Keys, 1991). Indeed, numerous events in finance and economics have been explained through a bubble metaphor, with Garber (1990) describing examples such as the Mississippi Bubble (1719-20) and the closely-connected South Sea Bubble resulting in The Bubble Act (1720). Cargill et al. (1997) provide a more recent example of Japan’s ‘bubble economy’ of the 1980s and Cellan-Jones (2001) recalls the ‘dot.com bubble’ at the turn of the twenty first century. In these specific examples, the bubble metaphor is used to explain (typically irrational) speculative in markets with ‘boom and bust’ characteristics (Harris, 1994). Metaphor then “encourages us to think and act in new ways. It extends horizons of insight and creates new possibilities” (Morgan, 1997, p. 351).

Whilst the use of metaphor to convey meaning and understanding is widespread and intuitively attractive, Beyer (1992, p. 467) cautions that “to employ a metaphor is useful only if we learn something new from doing so.” Furthermore, there are drawbacks and reliability issues, especially through the conveyance of unintended meanings along with intended ones (Beyer). Ramsay (2004) suggests that interpretation can be unreliable when characteristics are transferred from source (*ie*. bubble) to target (*ie*. confidentiality) domains; recommending that esoteric source domains should be avoided in preference for commonplace or banal, well-understood sources (as in this case). To facilitate the metaphoric comparisons (Glucksberg and Keysar, 1993) and categorical ‘matching’ process from bubble to confidentiality, we reflected on cases involving high levels of confidentiality that we have been directly involved in over recent years (including equipment developments for Olympic athletes and global merger and acquisition integration projects).

To complement the conceptual aspects of using metaphor, we draw on the principles of biomimetics to ensure that the imagery of the bubble trope has embodied the key features of the meaning it is aiming to convey. Biomimetics is the systematic transfer of concepts from the natural world in order to solve, typically, engineering and material science problems (Vincent, 2003). Biomimicry has also informed the development of organizational structures through observing the social behaviour of ant and bee colonies; and information technology design has been inspired through mimicking biological processes (Sørensen, 2004). In a related sense, ‘borrowing’ theory from one discipline to inform developments in another is commonplace (see Floyd, 2009). Indeed, Zahra and Newey (2009, p. 1070) state that “focussing on the intersection of fields and disciplines offers an important opportunity to theorize in ways that challenge, reframe and redefine core issues in a field/discipline”. In this paper, we are bringing together theories and concepts from management, psychology and the physical and social sciences in order to advance our understanding of confidentiality.

Metaphorically, the ideal scenario would be to maintain the integrity of the bubble, *ie*. maintain the confidentiality period until it is no longer required. If, however, a breach is imminent, then an understanding of the underlying forces, their limits and the ultimate failure mechanism becomes of interest, *ie*. how to avoid a breach.

**3. Conceptual Mapping of Bubble Characteristics to Confidentiality**

Drawing on general thermodynamics texts (*ie*. Çengel and Boles, 2010) and more specific ‘bubble dynamic’ research (*ie*. Feng and Leal, 1997; Plesset and Prosperetti, 1977; Reissner, 1956), we approach the theoretical development in two phases. Firstly, looking at how a bubble forms and potentially grows (metaphorically mapping this to establishing and ‘stressing’ confidentiality); and secondly, how a bubble may burst (mapping to breaches of confidentiality).

*3.1 Bubble Creation and Growth*

We consider a type of bubble enclosing a quantity of ideal gas by a membrane, such as that created by a soap solution. In exploring the bubble creation processes, we need to consider its key global properties and those acting upon it (see Figure 1); these being the mass *M* of its contents, radius *r*, volume *V*, internal pressure (*Pint*), and a measure of its energy represented by temperature *T*. For the purposes of developing the analogy, we will ignore the perturbations in shape and will assume the bubble will remain spherical. Hence,



and



---------------------------------

Insert Figure 1 about here

---------------------------------

The gas within the bubble has an internal energy which will increase, according to the first law of thermodynamics, in response to the total heat added (*Q*). The next significant relationship at this stage is derived by Boyle’s gas lawwhich incorporates pressure *P*, volume *V* and temperature *T*:



where *n* is the ‘amount of substance’ of the gas sample and *R* is the gas constant (both of which need not concern us in this illustration). The physical volume of the bubble will grow, contract or remain in stasis as determined by fundamental conservation equations of mass, momentum and energy. Volume and pressure are conjugate pairs, with pressure being the generalized force which can be changed by a rise in temperature (*T*). As the internal pressure (*Pint*) increases the volume will increase since the bubble wall has some elasticity (*ie*. the bubble will grow in size). The bubble will then stabilize once all forces are in equilibrium as per the combined gas law:



*3.2 From Bubble to Confidentiality: The Creation and Growth Phases*

As discussed earlier, we are drawing on metaphor and biomimetics in order to gain insights into the phenomenon of confidentiality. To this end, we are not looking for literal transcriptions, but an idea of the forces at play and their interactions. In transposing the characteristics of a bubble to a confidential scenario, we start by proposing the following equivalents in Table 1:

---------------------------------

Insert Table 1 about here

---------------------------------

Building on the process of creating a bubble, we suggest that the mass of gas inside the bubble relates to the ‘mass’ of confidential information and the individuals who are protecting that information are likened to the molecules of soap solution which make up the bubble membrane. These ‘guardians’ form a barrier between the enclosed confidential information inside the bubble and those ‘outsiders’ who seek to gain access. Therefore, as the guardians generate confidential information (*Wmech*) there is a degree of internal communication (*Q*) which results in an increase in the criticality (*T*) of maintaining confidentiality (metaphorically ‘*things hotting up*’ or ‘*feeling the heat*’ when the situation becomes more ‘agitated’ or ‘excited’). From (3), we can now see that the internal pressure (*Pint*) on guardians to manage the confidential situation will also rise. At this stage, without considering failure modes of the bubble for now, we posit that the embedded value of the system (*V*) will increase in response to the pressure until a point when stasis will be reached as suggested by (4). It is worth emphasizing that pressure, volume and temperature are in constant flux and change in order to reach equilibrium. As the bubble grows though, (1) and (2) show that the total exposure to outsiders (*S*) also increases, as does the related risk of a breach (*r*). These metaphorically transposed attributes and processes are summarized in Figure 2:

---------------------------------

Insert Figure 2 about here

---------------------------------

*3.3 Failure Mechanisms of a Bubble*

Having explored the mechanism behind creating a bubble and how it may grow in size, we now turn to the potential failure mechanisms of what is after all a fragile entity. The behaviour of a bubble placed in an environment will be determined by the properties of the membrane. If the membrane has a fixed mass *m* and its thickness *t* is small compared to the radius *r* of the bubble, then the limiting size of the bubble will be determined by the maximum stress *σ* (derived from force/area) that can be carried by the membrane. We now differentiate the failure modes into three distinct components, although all three are connected to the maximum stress that the membrane can withstand (see Figure 3 for a summary of the key attributes involved in the failure modes of a bubble).

---------------------------------

Insert Figure 3 about here

---------------------------------

Firstly, as the bubble continues to grow in size, the stress increases in the membrane and deformation will occur in the form of strain ε = Δ*t*/*to*, where Δ*t* is the change in membrane thickness and *to* is the original membrane thickness. As the bubble expands (+*T* → +*P* → +*V*), the thickness (*t*) of the bubble membrane will reduce as its mass *m* is conserved and so *σ* increases further (since the surface area of the membrane cross-section reduces). At some stage, *σ* will reach a critical level (*σ*crit) coinciding with the yield stress of the membrane material. The material then starts to stretch non-elastically and is unable to reach equilibrium, resulting in a catastrophic failure.

Secondly, a soap bubble membrane experiences decay through evaporation throughout its lifecycle. Such a process thins the bubble membrane until a point where the yield stress (*σ*crit) is reached; again resulting in catastrophic failure which can occur even when the internal properties are in stasis and the bubble’s size remains constant. Similarly in a growing bubble, evaporation of the membrane material will hasten the onset of failure.

Finally, it is worth noting that an homogeneous failure will occur simultaneously everywhere on a spherical surface; however, material variations in the membrane thickness and/or the presence of a stress raiser (*eg*. analogous with a pin or sharp edge) will cause an explosive rupture. This type of failure can occur at any stage of the bubble’s lifecycle irrespective of its size or dynamic.

*3.4 From Bubble to Confidentiality: Exploring the Failure Modes*

In considering the ‘confidentiality bubble’ failure mechanisms, it is the condition of the membrane interface that presents the greatest opportunity to consider possible mimicking, and we propose further similes in Table 2:

---------------------------------

Insert Table 2 about here

---------------------------------

Taking the descriptions in Tables 1 and 2, we can now piece together the actions and interactions in the run-up to a breach in confidentiality (see Figure 4). We equate the bubble membrane to being a well bonded team of guardians metaphorically joining together to form a cohesive surface tension, thereby encircling and protecting the information (note: whilst four guardians are shown in a small segment of the bubble, they are envisaged to form a complete ‘enclosure’ around the confidential information. This would be the case whenever the guardians numbered two or more). Again metaphorically, the guardians can be viewed as the molecules within the membrane material; with mutual *trust* being the equivalent of atomic forces or bonds holding them together to form a barrier of a certain ‘thickness’, depending on the levels of trust between them.

---------------------------------

Insert Figure 4 about here

---------------------------------

In this context, trust is considered to be a multidimensional construct (*eg*. Lewicki et al., 2006; Mayer et al., 1995; Rousseau et al., 1998) representing the basic assumption that an individual is willing to be vulnerable to the intentions or behaviours of another based on the expectation that the trustee (the one who is being trusted) will behave in a reciprocal manner (Mayer et al., 1995). Mayer et al.’s (1995) model advocates three dimensions of perceived trustworthiness that are required antecedents for trust to develop between two parties. The first is belief in another’s *ability* or domain-specific knowledge; in this case it may relate to whether individuals are perceived by others to have the ability to not disclose sensitive information. The second dimension, *benevolence*, is the extent to which the trustor believes that the trustee will act in their own best interests or for the good of the collective group. Applied to a confidentiality bubble, this would relate to whether guardians would perceive others to be working for the good of the group (*eg*. keeping the confidentiality bubble intact), rather than having their own agenda or mixed motives for being there (Jarvenpaa and Majchrzak, 2008). The third is the perception of *integrity* where one believes that the trustee will adhere to a set of principles, and behave in accordance with their promises. Again, within this context, such a belief is crucial to the development of trust as it serves as a reliability measure. Mayeret al. (1995) affirm that trust is more likely to develop when all three dimensions of trustworthiness are high; however lack of belief in any one may weaken actual trust development, affecting subsequent behaviours and outcomes. Levels of trustworthiness can therefore oscillate according to one’s propensity to trust as well as the particular context or task for which trust is needed.

Within any teamwork context one can anticipate the presence of multiple motives. In relation to a confidentiality bubble therefore, we consider that trust serves as an organizing principle (McEvily et al., 2003); its function being to structure and mobilize the social networks to help keep the bubble intact as well as acting as a potential diffuser of stress in many circumstances. At the boundary interface, there exists the potential for complex interactions involving trust, reciprocity, risk and ‘reward’ between both guardian:guardian (G:G) and guardian:outsider (G:O) axes. We therefore posit that levels of trustworthiness will have an impact on the development of trust which will act as a trigger for how guardians subsequently engage in risk-taking actions and how they behave within the bubble (Mayer et al., 1995).

From earlier discussions, there are three potential modes for the bubble to burst, thereby releasing the contents to the outside environment. Having identified the remaining similes and the central role of trust, these breach modes are now mapped to the confidentiality scenario.

3.4.1 Breach through exceeding the membrane yield stress in an expanding bubble

As the amount of value in the system increases, the risk of a breach (radius) is also deemed to increase as the exposure (surface area) also increases. This expansion causes a rise in stress and strain amongst the guardians, especially if moral dilemmas are present, trying to pull them apart and effectively ‘thinning’ or straining trust levels. As discussed above, trust is central to articulating the membrane dynamics of the bubble as it can be likened to the ‘glue’ that serves two purposes. First it holds those in the bubble wall together in keeping them in their confidentiality state. Second, depending on the type and strength of trust developed, it will influence the length of time the bubble can be sustained. So trust can be conceptualized as a potentially moderating force against any ‘stress’, or internally generated risks (Barber, 2005), that may occur.

From a decision-making perspective - either through rationality (Simon, 1955), Prospect Theory (Kahneman and Tversky, 1979) or Expected Utility Theory (von Neumann and Morgenstern, 1944) for instance - guardians are weighing up the potential rewards versus risks or sanctions (both economic and non-economic) of remaining within the ‘in-group’ against leaving and joining the ‘out-group’, resulting in a breach of confidentiality. At the same time, trust assessments of ability, benevolence and integrity are made in each individual G:O axis for accurate information and assurances of anonymity. We propose that such assessments may be made either consciously or sub-consciously, along the lines of principal:agent models driving self-interest behaviour (De Cremer et al., 2011) together with a measure of risk (Özer et al., 2011). Belief in a guardian’s ability to keep information secure may be undermined if levels of benevolence and integrity are low as this could suggest that person has mixed motives: *eg*. agrees in principle to confidentiality, but due to a change in circumstances may decide to break the agreement and leak information in order to serve their own ends rather than for the benefit of the collective. This leads to the first research proposition:

P1: Belief in a guardian’s ability to keep information secure will be undermined when levels of benevolence and integrity are low.

At some point in the expansion of the bubble then, when the value of the information generates stresses that coincide with the critical or yield stress (*σ*crit) – which could be a measure of loyalty - the trust bonds between two or more guardians will break. The membrane is only as strong as its weakest link and we might colloquially talk about *stretching trust to breaking point*. At this point, the membrane is stressed beyond its ability to recover from elastic deformation and the system is destined for failure. This is captured in the second research proposition:

P2: The trust bonds between guardians will break when the value of the information generates stresses that surpass the yield stress (*σ*crit).

3.4.2 Breach through evaporation of G:G trust levels

The second mode of breach is very similar to the first; except that here the team have completed (or halted for some reason) their work on developing confidential information (*ie*. the bubble size remains constant). The same dynamics are at play except that the longer the information is held in a confidential state, the more the G:G trust may evaporate as there is a greater time span for G:O trust to develop in its place, effectively thinning the bubble membrane. If the situation is allowed to continue, the G:G trust levels may thin to a point where the ‘yield stress’ is reached (*σ*crit) and a guardian would leak information. It is worth noting that evaporation is taking place throughout the bubble’s lifecycle and has the potential to also thin G:G trust levels in the first mode outlined above. The main reason for separating it out here is to illustrate the importance of timeliness in dealing with confidential information, and how a bubble in stasis can still be breached. Harwood (2006) identified both these forms of breach as a ‘trading transfer’, whereby guardians of confidential information would trade off the risks and rewards of breaching confidentiality versus those associated with maintaining it. This leads to the third research proposition:

P3: When the rewards or entitlements outweigh the risks or sanctions, and G:O trust supersedes G:G trust levels at an individual level, a breach in confidentiality may occur.

3.4.3 Breach via a ‘stress raiser’

Having explored the breach mechanisms due to the bubble being stressed beyond the material strength of the membrane, we now identify the equivalents of a ‘sharp object’ or ‘stress raiser’ immediately breaching the bubble, irrespective of its size or rate of evaporation. In addition to the ‘trading transfer’ mechanism explained above, Harwood (2006) also identified the following avenues for confidential information transfer to ‘outsiders’, despite there being a non-disclosure agreement in place:

* *Deliberate transfers* relate to confidential information being leaked in order to prepare those who may be impacted by forthcoming change or announcements. Deliberate transfers can also result from ‘organizational gossip’ (Michelson et al., 2010); with Mills (2010) suggesting this is a central part of sensemaking and social exchange in change-related communication.
* *Ethical transfers* occur when information is deliberately leaked where unethical behaviour has occurred, is occurring or is likely to occur, *ie*. whistle-blowers, or where professional guidelines require disclosure in the case of imminent self-harm. The Public Interest Disclosures Act 1998 (or ‘Whistle-blowers’ Act) applies to individuals in the UK raising concerns over malpractice in organisations. Confidentiality (gagging) clauses in employment contracts and severance agreements are deemed void under the terms of the Act.
* *Accidental transfer* happens when information is transmitted, either verbally or electronically, in error.
* *Illegitimate transfer*, or misappropriation, occurs when information is stolen through deception, covert surveillance, hacking or interception, as is common in cases of industrial espionage (see Blair et al., 2013 or Donilon, 2013 for examples).

Each of these can be viewed as a ‘stress raiser’ resulting in an immediate breach of the confidentiality ‘membrane’, irrespective of the size of bubble at the time of rupture or the degree of trust amongst the guardians. The first three stress raisers operate outwards from the inside of the bubble; the last one (illegitimate transfer) from the outside in. This leads to the fourth research proposition:

P4: Stress raisers (through deliberate, ethical, accidental or illegitimate transfers) will result in an immediate breach of confidentiality.

*3.5 Preventing a premature breach of confidentiality*

Having identified the potential modes of a breach, we offer some further propositions surrounding the prevention of the ‘bubble’ from bursting prematurely:

**Manage the volume**: minimizing the channels and volume of internal communication (*ie*. hold information on a ‘need to know’ basis and minimise any ‘agitation’ or ‘excitement’) will limit the size of the bubble thereby reducing exposure, risk and stress placed on the guardians.

P5: Minimising channels and volume of internal communication will reduce the probability of confidential information being leaked.

**Maintain trust levels**: Steele’s (1989) ‘clique communication model’ suggests that the more people in the clique, the higher the probability of information being leaked. Our model supports this view as each new member presents another trust ‘link’ which can potentially be broken when the yield stress is reached. A measure of trust as perceptions of ability, benevolence, integrity and propensity could be taken before individuals become managers/team members. Individuals would therefore be chosen not just for their domain-specific knowledge but also for their trustworthiness and ability to trust. Once signed up, work on strengthening the trust between guardians should be on-going. Rather than running (usually one-off) team-building activities at the start of a project or activity, our model shows the importance of periodically reinforcing or replenishing trust through on-going team-building activities. Metaphorically, this would increase the thickness of the membrane, enabling it to sustain higher levels of stress and strain. Constructively training guardians in team skills that can help promote trust will assist in the ‘art’ of working confidentially (Prichard and Ashleigh, 2007) and provide ‘collective competence’ (Melkonian and Picq, 2010). Depending on the context and number of signatories, it may also help to establish a mentoring system to pair up experienced guardians with those for whom working with confidential information is a new experience. Since the membrane is constantly evaporating, it is also a useful reminder to deal with confidential situations swiftly, with minimal delay.

P6: Proactively increasing trust levels between guardians will reduce the risk of confidential information being leaked.

**4. Summary and Conclusions**

Confidentiality can be a business critical issue and a source of competitive advantage if strongly maintained. It is therefore surprising to find so little prior research on the topic in management academic literature. The ‘bubble’ model proposed in this paper, together with the propositions and recommendations, provide managers with a theoretical ‘frame’ which should aid the visualization and articulation of the issues faced when preventing a breach of restricted information.

The ‘confidentiality bubble’ appears to be intuitively appealing and we envisage applications across a wide range of settings. More complex models could be explored which incorporate more physical variables (entropy for example), or indeed different types of bubbles (*eg*. vapour bubbles with permeable membranes) or even foam. We are though cautious against over-complicating the theoretical model with too many variables at this stage; with Steele (1989, p. 243) stating that “such analyses are best deferred until one is confident that the simplest analytic models are well understood, both for their shortcomings and their strengths.” We are also mindful of the need to avoid the pitfalls of overly transcribing attributes from source to target in a literal sense when using metaphors (Ramsay, 2004). Therefore, the next stage will be to design and conduct an experiment in order to empirically test the robustness and validity of the ‘confidentiality bubble’ model described here (and the propositions based on the key attributes of internal communication, ‘agitation’, ‘excitement’, criticality, internal pressure, embedded value, trust, yield stress and stress raisers), before adding further complexity if necessary.

Until now, the topic of confidentiality has received very little coverage in the management literature. Given that most organisations deal with commercially sensitive information, with far-reaching consequences from a breach in confidentiality (especially in ‘restricted’ sectors such as nuclear power or defence), this is a significant omission. We believe this paper could be the catalyst for further developments in this critical area.

**References**

Anand, K.S., & Goyal, M. (2009). Strategic Information Management Under Leakage in a Supply Chain. *Management Science*, *55*, 438-452.

Barber, R.B. (2005). Understanding internally generated risks in projects. *International Journal of Project Management, 23*, 584-590.

Beyer, J.M. (1992). Metaphors, Misunderstandings, and Mischief: A Commentary. *Organization Science*, *3*, 467-474.

Blair, D.C., Huntsman, J.M, Barrett, C.R., Gorton, S. Lynn III, W.J. Wince-Smith, D. & Young. M.K. (2013). *The IP Commission Report*, Available: <http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf>, last accessed 15th July 2013.

Cain, P. (1998). The Limits of Confidentiality. *Nursing Ethics*, *5*, 158-165.

Capelli, S., & Jolibert, A. (2009). Metaphor’s Validity in Marketing Research. *Psychology & Marketing*, *26*, 1079-1090.

Cargill, T.F., Hutchison, M.M., & Ito, T. (1997). *The Political Economy of Japanese Monetary Policy*. Massachusetts: MIT Press.

Cellan-Jones, R. (2001). *Dot.bomb: the rise & fall of dot.com Britain*. London, UK: Aurum Press Ltd.

Çengel, Y.A., & Boles, M.A. (2010). *Thermodynamics: an Engineering Approach* (7th ed.). McGraw-Hill.

Cornelissen, J.P., Holt, R., & Zundel, M. (2011). The Role of Analogy and Metaphor in the Framing and Legitimization of Strategic Change. *Organization Studies*, Published online before print, November 1, 2011, DOI: 10.1177/0170840611425729.

Cornelissen, J.P., & Kafouros, M. (2008). Metaphors and Theory Building in Organization Theory: What Determines the Impact of a Metaphor on Theory? *British Journal of Management*, *19*, 365-379.

De Cremer, D., van Dick, R., Tenbrunsel, A., Pillutla, M., & Murnighan, J.K. (2011). Understanding Ethical Behavior and Decision Making in Management: A Behavioural Business Ethics Approach. *British Journal of Management*, *22*, S1-S4.

Donilon, T. (2013). *The United States and the Asia-Pacific in 2013*. The Asia Society, New York, 11th March 2013, Available: <http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a>, last accessed 15th July 2013.

Feng, Z.C., & Leal, L.G. (1997). Nonlinear Bubble Dynamics. *Annu. Rev. Fluid. Mech.,* *29*, 201–243.

Floyd, S.W. (2009). ‘Borrowing’ Theory: What Does This Mean and When Does It Make Sense in Management Scholarship? *Journal of Management Studies*, *46*, 1057-1058.

Garber, P.M. (1990). Famous First Bubbles. *The Journal of Economic Perspectives*, *4*(2), 35-54.

Gaumnitz, B.R., & Lere, J.C. (2002). Contents of Codes of Ethics of Professional Business Organizations in the United States. *Journal of Business Ethics*, *35*, 35-49.

Gewirth, A. (2001). Confidentiality in child-welfare practice. *Social Service Review*, *75*, 479-489.

Glucksberg, S. (2003). The psycholinguistics of metaphor. *Trends in Cognitive Sciences*, *7*, 92-96.

Glucksberg, S., & Keysar, B. (1993). How metaphors work. In A. Ortony (Ed.) *Metaphor and Thought* (2nd ed.) (pp. 401-424). Cambridge, UK: Cambridge University Press.

Harris, R. (1994). The Bubble Act: Its Passage and Its Effects on Business Organization. *The Journal of Economic History*, *54*, 610-627.

Harwood, I.A. (2006). Confidentiality constraints within mergers and acquisitions: gaining insights through a 'bubble' metaphor. *British Journal of Management*, *17*, 347-359.

Harwood, I.A., & Ashleigh, M.J. (2005). The impact of trust and confidentiality on strategic organizational change programmes: a case study of post-acquisition integration. *Strategic Change*, *14*, 63-75.

Hook, M.K., & Cleveland, J.L. (1999). To tell or not to tell: Breaching confidentiality with clients with HIV and AIDS. *Ethics & Behavior*, *9*, 365-381.

Jarvenpaa, S.L., & Majchrzak, A. (2008). Knowledge collaboration among professional protecting national security: Role of transactive memories in ego-centred knowledge networks. *Organization Science,* *19*, 260-276.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision Under Risk. *Econometrica*, *47*, 263-291.

Keys, P. (1991). Operational Research in Organizations: a Metaphorical Analysis. *Journal of the Operational Research Society*, *42*, 435-446.

Lewicki, R.J., Tomlinson, E.C., & Gillespie, N. (2006). Models on interpersonal trust development: Theoretical approaches, empirical evidence and future directions. *Journal of Management*, *32*, 991-1002.

Li, L. (2002). Information Sharing in a Supply Chain with Horizontal Competition. *Management Science*, *48*, 1196-1212.

Li, L., & Zhang, H. (2008). Confidentiality and Information Sharing in Supply Chain Coordination. *Management Science*, *54*, 1467-1481.

Majchrzak, A., & Jarvenpaa, S.L. (2004). Information Security in Cross-Enterprise Collaborative Knowledge Work, *E:CO*, 6, 4-8.

# Masters, B. (2012). *Credit Suisse trader fined after game of ‘charades’*, available: <http://www.ft.com/cms/s/0/f44f0870-6d07-11e1-ab1a-00144feab49a.html#axzz2YqL4uYkL>, last accessed 12th July 2013.

Mayer, R.C., Davis, J.H., & Schoorman, F.D. (1995). An integrative model of organizational trust. *Academy of Management Review*, *20*, 709-734.

McEvily, B., Perrone, V., & Zaheer, A. (2003). Trust as an Organizing Principle. *Organization Science,* *14*, 91-103.

Melkonian, T., & Picq, T. (2010). Opening the “Black Box” of Collective Competence in Extreme Projects: Lessons From the French Special Forces. *Project Management Journal, 14*, 79-90.

Michelson, G., van Iterson, A., & Waddington, K. (2010). **Gossip in Organizations: Contexts, Consequences, and Controversies,** Group & Organization Management, 35, 371-390.

Milberg, S.J., Smith, H.J., & Burke, S.J. (2000). Information Privacy: Corporate Management and National Regulation, *Organization Science*, *11*, 35-57.

Mills, C. (2010). **Experiencing Gossip: The Foundations for a Theory of Embedded Organizational Gossip,** Group & Organization Management, 35, 213-240.

Morgan, G. (1997). *Images of Organization*. Thousand Oaks, CA: Sage Publications.

Ortony, A. (ed.) (1993). *Metaphor and Thought* (2nd ed.). Cambridge, UK: Cambridge University Press.

Özer, Ö., Zheng, Y., & Chen, K. (2011). Trust in Forecast Information Sharing. *Management Science*, *57*, 1111-1137.

Phillips, K.W., Rothbard, N.P., & Dumas, T.L. (2009). To disclose or not to disclose? Status distance and self-disclosure in diverse environments. *Academy of Management Review*, *34*, 710-732.

Plesset, M.S., & Prosperetti, A. (1977). Bubble dynamics and cavitation. *Annu. Rev. Fluid. Mech.*, *9*, 145-185.

Prichard, J.S., & Ashleigh, M.J. (2007). The effects of team-skills training on transactive memory and performance. *Small Group Research*, *38*, 696-726.

Pouillot, P. (2011). Data Security, *Strategic Risk Executive Report*, Nov. 2011, 1-13.

Rae, W.A., Sullivan, J.R., Peña Razo, N., George, C.A., & Ramirez, E. (2002). Adolescent health risk behavior: When do pediatric psychologists break confidentiality? *Journal of Pediatric Psychology*, *27*, 541-549.

Ramsay, J. (2004). Trope Control: The Costs and Benefits of Metaphor Unreliability in the Description of Empirical Phenomena. *British Journal of Management*, *15,* 143-155.

Ramsay, J., & Croom, S. (2008). The impact of evolutionary and developmental metaphors on Purchasing and Supply Management: a critique. *Journal of Purchasing & Supply Management*, *14*, 192-204.

Reissner, E. (1956). A Note on Membrane and Bending Stresses in Spherical Shells. *Journal of the Society for Industrial and Applied Mathematics*, *4*, 230-240.

Rousseau, D.M., Sitkin, S.B., Burt, R.S., & Camerer, C. (1998). Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review*, *23*, 393-404.

Rukšėnas, R., Curzon, P., & Blandford, A. (2008). Modelling and analysing cognitive causes of security breaches. *Innovations in Systems and Software Engineering*, *4*, 143-160.

Shing, M., Shing, C., Chen, K.L., & Lee, H. (2009). Confidentiality modelling and simulation and validation in a simplified database access. *International Journal of Computational Biology and Drug Design*, *2*, 252-263.

Simon, H.A. (1955). A Behavioral Model of Rational Choice. *The Quarterly Journal of Economics*, *69*, 99-118.

Sitkin, S.B., & Roth, N.L. (1993). Explaining the limited effectiveness of legalistic ‘remedies’ for trust/distrust. *Organizational Science*, *4*, 367-392.

Smith, S.P. (2000). Are you protecting your patients' confidentiality? *Nursing Economics*, *18*, 294.

Sørensen, M.H. (2004). The Genealogy of Biomimetics: Half a Century’s Quest for Dynamic IT. In A.J. Ijspeert, M. Murata & N. Wakamiya (Eds.), *Biologically Inspired Approaches to Advanced Information Technology* (pp. 496–512). Heidelberg: Springer Berlin.

Steele, J.M. (1989). Models for Managing Secrets. *Management Science*, *35*, 240-248.

Vincent, J.F.V. (2003). Biomimetic modeling. *Philosophical Transactions: Biological Services*, *358*, 1597-1603.

von Neumann, J., & Morgenstern, O. (1944). *Theory of Games and Economic Behavior*. Princeton, NJ: Princeton University Press.

Waistell, J. (2006). Metaphorical mediation of organizational change across space and time. *Journal of Organizational Change Management*, *19*, 640-654.

Waistell, J. (2007). Metaphorical Perspectives of Organisational Values. *Culture and Organization*, *13*, 83-97.

WMA. (2009). *WMA Medical Ethics Manual* (2nd ed.). Available: <http://www.wma.net/en/30publications/30ethicsmanual/index.html>, last accessed 22nd July 2013.

Zahra, S.A., & Newey, L.R. (2009). Maximizing the Impact of Organization Science: Theory-Building at the Intersection of Disciplines and/or Fields. *Journal of Management Studies*, *46*, 1059-1075.

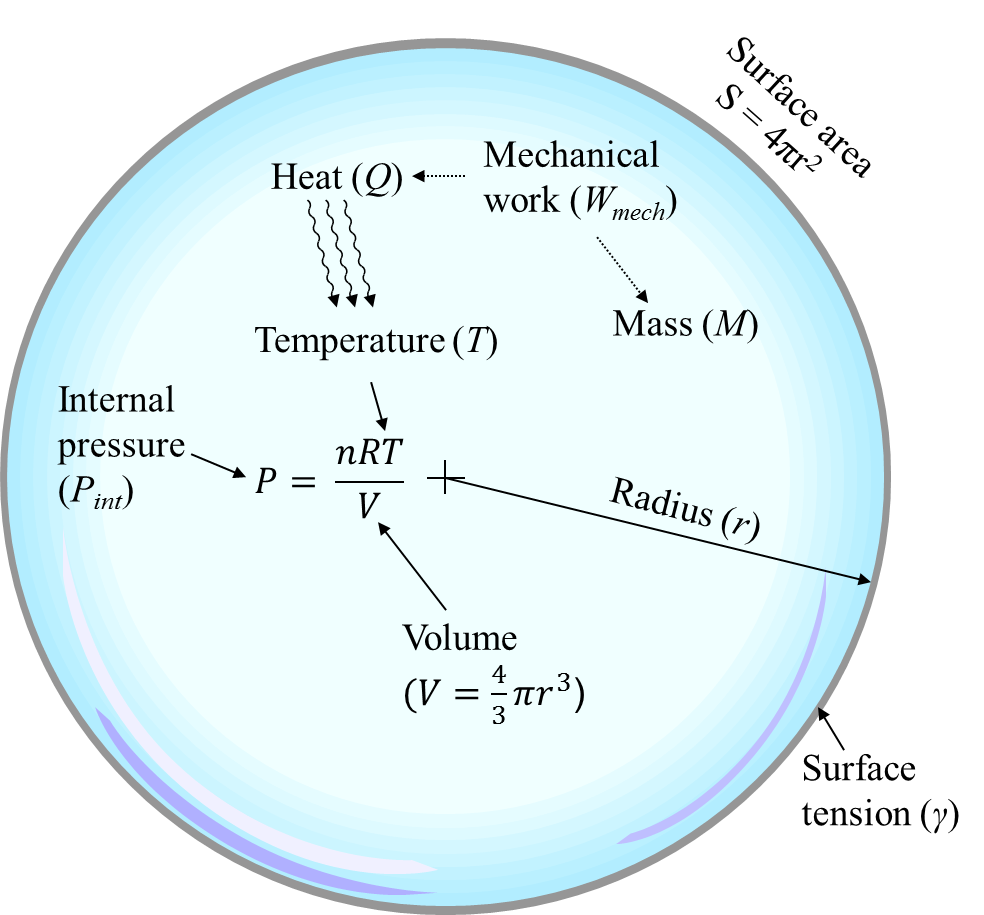
**Table 1: Attributes Relating to the Bubble Creation and Growth Phases**

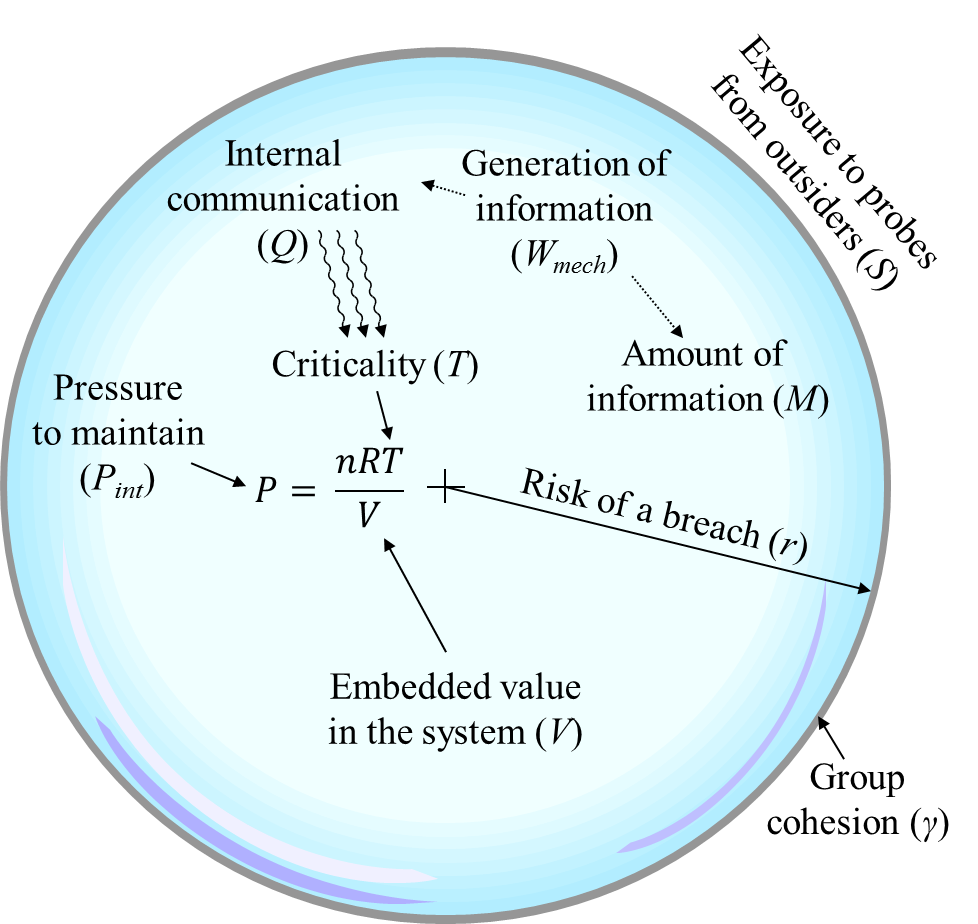
|  |  |
| --- | --- |
| **Bubble attribute** | **Equivalent attribute of confidentiality** |
| Membrane material  Mechanical work (*Wmech*)  Mass of the ideal gas *M*  Heat *Q*  Temperature *T*  Internal pressure *Pint*  Volume *V*  Surface tension γ  Surface area *S*  Radius *r* | The individuals who are entrusted to keep the confidential information a secret, *ie*. the ‘guardians’ who form a barrier preventing outsiders from accessing the confidential information.  The generation of information by the guardians.  The amount of information held by the guardians *ie*. a ‘*mass of information*’.  The rate of internal communication about the information.  A measure of the criticality of maintaining confidentiality.  The pressure exerted on each of the guardians to maintain confidentiality; in other words, to *feel the pressure* of maintaining or managing confidentiality.  The embedded value within the system.  Group cohesion, *ie*. the guardians *all pulling together*.  The overall exposure to probes from outsiders.  The risk of a breach in confidentiality. |

**Table 2: Attributes Relating to the Failure Mechanisms**

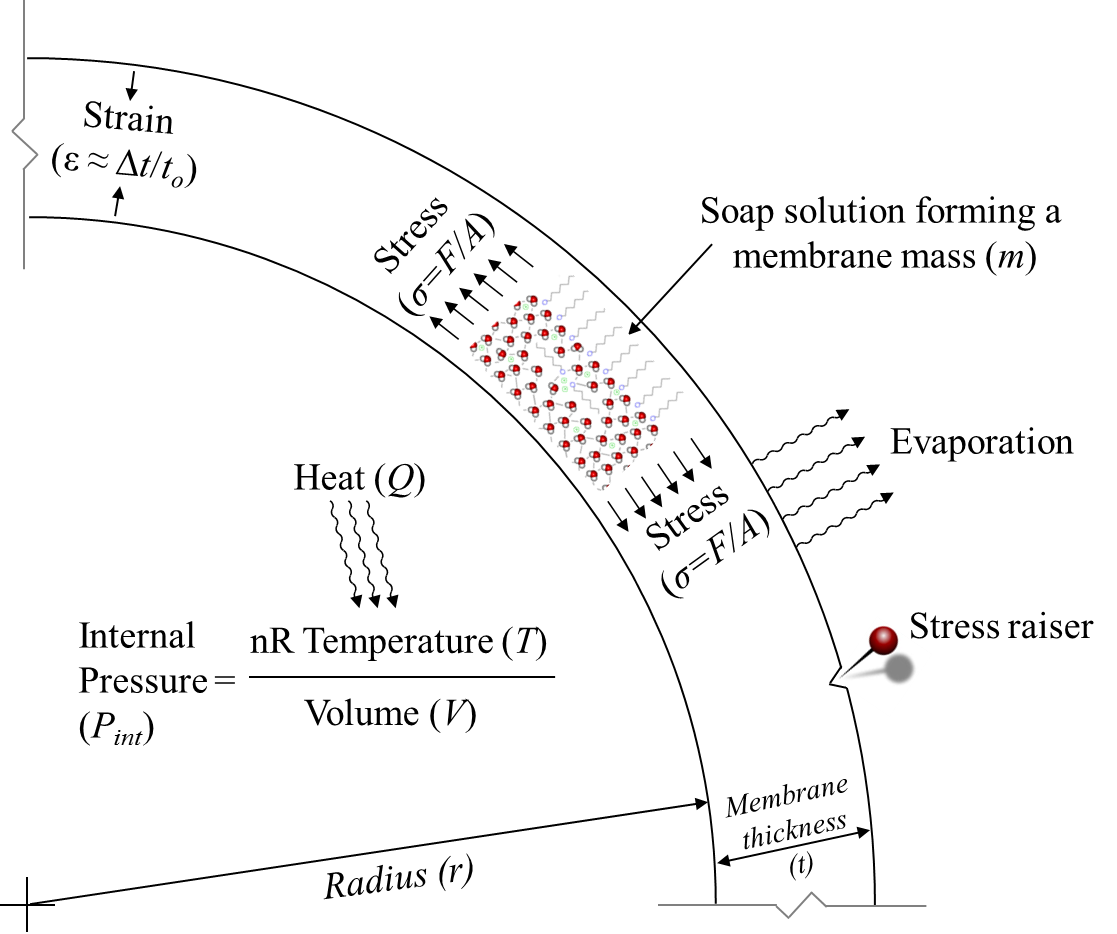
|  |  |
| --- | --- |
| **Bubble attribute** | **Equivalent attribute of confidentiality** |
| Membrane mass *m* | The number of guardians. |
| Membrane thickness *t* | The level or degree of trust between the guardians. |
| Membrane evaporation | A reduction in intra-guardian trust over time. |
| Stress *σ* = force/area | The pressure experienced by the guardians to bring about a breach in confidentiality. |
| Strain ε ≈ Δ*t*/*to* | The resultant deformations on allegiance and intra-group trust as guardians are being pulled apart. Measured by the change in trust (membrane thickness) over the original level of trust. |
| Stress raiser | An external action or interaction that stresses the trust bonds between guardians. |
| Critical (yield) stress *σ*crit | The point at which trust breaks and confidential information is leaked. |

**Figure 1: Key Attributes of a Bubble**

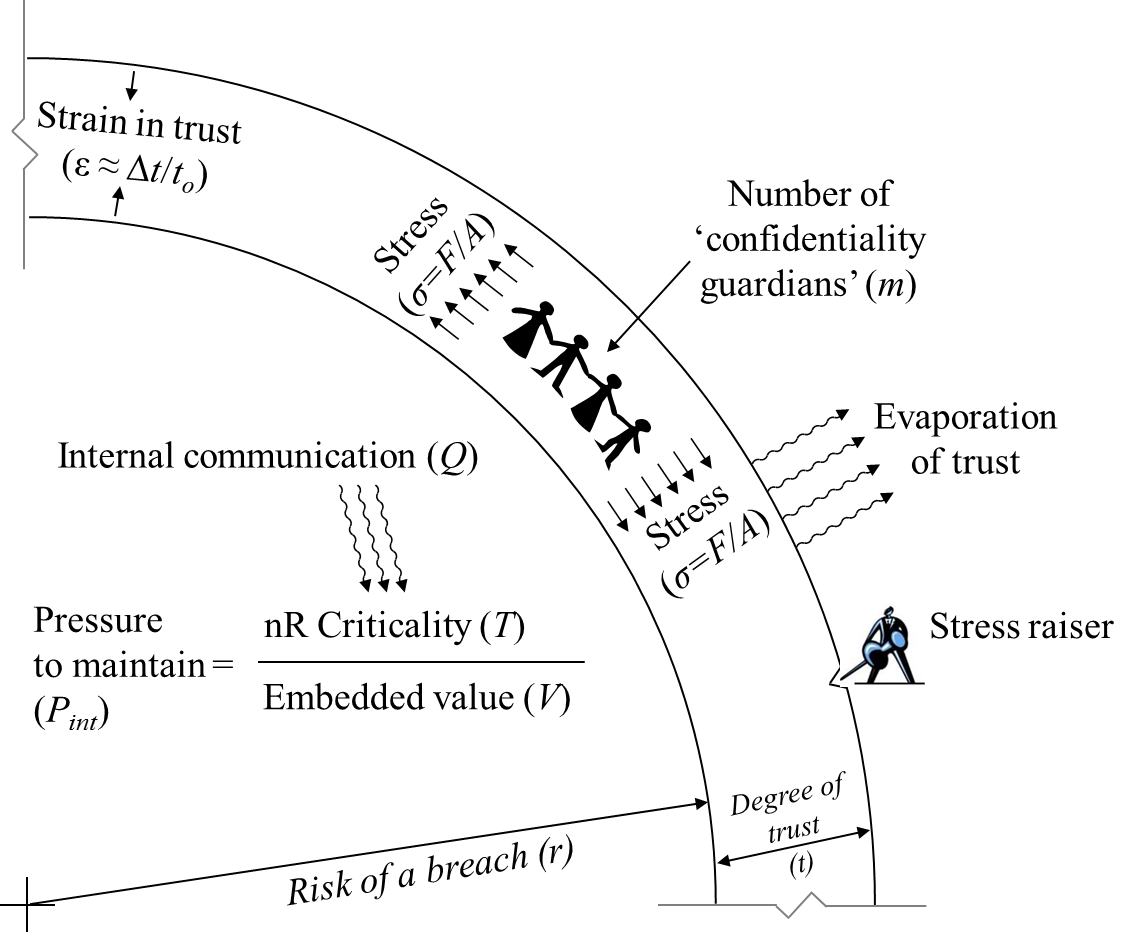
**Figure 2: Key Attributes of a ‘Confidentiality Bubble’**

****

**Figure 3: Cross-section of a Bubble Membrane Segment Showing key Attributes Contributing to Failure**

****

**Figure 4: Cross-section of a ‘Confidentiality Bubble’ Membrane Segment Showing key Attributes Contributing to a Breach**

****