Talking Out Both Sides of Your Mouth: Streamlining Communication via Metaphor

GIAC (GCIH) Gold Certification

Author: Josh More, jmore@starmind.org

Advisor: Mohammed Haron

Accepted: May 1st 2013

Abstract

As Security is a relatively new field, we are still learning how to communicate what we know with those outside of it. When communicating with non-experts, we often fall back on simplification and analogy to make our points understood. These techniques are fundamentally based on metaphor.

This paper explains how metaphors are classically used, drawing on works in the field of linguistic philosophy, communication theory and neuro-linguistic programming. It then explores classic metaphors used within the Security community, analyzing publicly-available incident reports. Finally, the paper proposes some techniques that can be used to discover metaphors that are likely to work, thereby streamlining communication with those outside the field.

This approach can make it easier to convey issues related to incidents quickly and accurately. It can be useful to streamline resource acquisition to implement technology or processes to prevent recurrence. It can be used to help educate junior co-workers and to report to management. Fundamentally, the proper use of metaphor can dramatically shorten communication cycles and free up time for action.

1. Introduction

Though we often agree as to what individual words mean, it is often true that complex ideas cannot be adequately described in a reasonable amount of time. As concepts build upon other concepts, it can take a very long time to raise individuals within a conversation to equivalent levels to produce a productive technical discussion. However, alternatives that allow for faster communication bring with them ambiguity. While such ambiguity of communication is part of the human condition, it can cause problems when rapid but highly technical communication is required. In activities such as incident management, it is often necessary to communicate with numerous stakeholders, none of which may be expected to grasp technical subtleties. As a result, it is common to lose time in explanation rather than spend it more profitably in discussing potential solutions.

This paper explores ways in which this communication may be better balanced, by focusing on one method of communication… metaphor. By understanding how metaphors function, better metaphors may be selected and used during crisis communication, shortening necessary discussion and allowing for faster resolution.

2. Introducing Metaphor

There are many definitions of metaphor. Fortunately, this is not a paper on linguistic philosophy, so the adoption of a strict definition is not required. Much of *Metaphors We Live By* (Lakoff & Johnson, 1980) is devoted to these subtleties. However, for this paper, the definitions from Dictionary.com will be generally sufficient:

noun

1. a figure of speech in which a term or phrase is applied to something to which it is not literally applicable in order to suggest a resemblance, as in “A mighty fortress is our God.” Compare mixed metaphor, simile (def 1) .

Josh More, jmore@starmind.org

2. something used, or regarded as being used, to represent something else; emblem; symbol.

("Dictionary.com,")

Specifically, the second definition is more suitable. By using metaphor, it becomes easier to discuss abstract concepts. Metaphor can also be used as a framework that constrains and guides discussion while simultaneously expanding the examples that can be used to explain abstract concepts.

A classic example from Lakoff and Johnson's work is "Argument as War", later revised to "Argument as Conflict" (Lakoff & Johnson, 1980). In this metaphor, arguments are cast in ways that call to mind language used to describe war and conflict:

- Your claims are *indefensible*.
- He *attacked* every weak point in my argument.
- His criticisms were right on *target*.
- I *demolished* his argument.

Thus, the relatively complex and amorphous concepts of working through disagreement to reach interpersonal resolution reference the more concrete concepts of physical conflict. This makes it easier to communicate concerns without necessitating perfect understanding of the specific situation being discussed.

2.1.How Metaphors Are Used

Metaphor is generally used everywhere, but specific metaphors are used in specific industries. As an industry matures, culture forms. More specifically, though, these cultures invent ways of communicating within themselves that create metaphors. These metaphors then enforce the emerging culture. (Morgan, 2006)

Metaphors, therefore, create and are created by culture. However, since they exist to guide understanding down a specific pathway, they can also hinder understanding. If the metaphors are poorly selected or if situations change from when they were first introduced, it can result in failure. Gareth Morgan's *Images of Organization* explores several different metaphors for companies and how they work, including: Machines, Organisms, Brains, Cultures and Political Systems. He also gives careful attention to the ways in which these metaphors would fail or break down when extended past their point of usefulness.

2.1.1.Metaphors as Communication Accelerators

It is a commonly held belief in the fields of Linguistics and Philosophy that the human brain requires metaphor to conceive complex thoughts and that; moreover, metaphors often cannot be replaced by factual statements (Ortony, 1975). Thus, metaphors form the way in which people think. Further research has shown that while the meaning of a metaphor will vary from person to person, the process is dynamic and contextual, with communication requiring the continuous alteration of the metaphor to maximize understanding (Zhou & Heineken, 2009).

In other words, as two or more individuals attempt to understand one another, they go back and forth, refining their metaphors until all parties reach agreement or communication appears impossible and is terminated. It is therefore reasonable to conclude that metaphors with more in common between those communicating are more likely to result in a more rapid understanding of a concept. Over time, individuals and cultures select metaphors that work for one another and can reinforce the culture while streamlining communication (Morgan, 2006).

Metaphors are not, however, perfect and do not always advance understanding.

2.1.2.Metaphor Breakdown

Metaphors can fail or "break down". Methods include metaphor conflict (Lakoff & Johnson, 1980) as well as the metaphor being overly restrictive or failing to extend as one might expect (Morgan, 2006).

Good examples of these can be seen in the security analogy project run by Scott Granneman in 2007. Consider the DDOS as Phone Calling metaphor, where a denial of service attack can be likened to a thousand people repeatedly calling a person's phone number. The metaphor has aged poorly as modern phones have blacklists and caller ID, so to make continue to function; the metaphor must be extended so that the person receiving the calls is thought of as a receptionist. (Granneman, 2007)

Since metaphors are abstractions by nature, each one will have one or more points of breakdown. Considering other metaphors from the security analogy project:

Metaphor	Where it fails
Adware as Paparazzi	Adware and the Paparazzi both make money by sharing data about the target. However, the Paparazzi are not reused for directly malicious purposes when their author wishes.
Anti-virus as Flu Shot	This metaphor can fail on cultural grounds. While the core of the metaphor is sound, the concept of vaccination has been increasingly attacked in Western culture. A mis-targeting of this metaphor to someone who is biased against vaccines could cause them to transfer that bias against anti-virus software as well.
Storage as Shelves	The Disk Storage as Row of Shelves metaphor is extended within the original site to include the concept of slack space. This implies a recognition that the core metaphor isn't up to the task to facilitating communication. The metaphor also suffers from age, as using it to discuss more modern file formats such as ext4 or zfs would require additional extension of the metaphor.

Josh More, jmore@starmind.org

Monoculture	The monoculture metaphor used to explain the risks of having all systems on a network run the same version of the operating system breaks down by not acknowledging the comparative difficulty of a farmer raising complementary crops versus a system administrator maintaining non-complementary operating systems. While there has been work done more recently to make it easier for operating systems such as Windows and Linux interoperate more easily, such has not always been the case. This metaphor has a secondary failure mode by failing to acknowledge that not all attacks are widely focused. Within this analogy, many attacks would focus on a particular plant (workstation) that is destined to be eaten by the farmer (network administrator). This extension stretches the limits of credulity, illustrating the breakdown of the metaphor.
Administrator as Superintendent	The root as home owner analogy positions an administrative user as a building superintendent and the unprivileged users as people living within the building. This metaphor breaks down when one realizes that in a real building, the rules are enforced socially whereas in an operating system, they are enforced technically. Thus, in a building, someone may intentionally kick down someone else's door or light a fire and burn down the entire building. A well-constructed operating system will prevent that.

These metaphors, and others from various security metaphor and analogy lists, can be considered along classic metaphor analysis lines and put into higher level "meta" grouping such as "virtual as physical", "technological as biological" or "control as social obligation". However, as one can see comparing the more general "monoculture"

metaphor to the more specific "storage as shelves", specific metaphors can function at a deeper level without extension. In other words, the closer a metaphor is to a target's background, the less metaphor extension is likely to get in the way of communication.

2.1.3.General vs Specific Metaphors in Information Security

Within information technology, metaphors abound. This may be because information technology has grown so quickly that entire generations do not have a firm grasp of the technology and must resort to analogy and metaphor to discuss it. Terms such as *information super highway* and metaphors such as *series of tubes* are used to explain the Internet and are accessible globally. (Gromov) (Kos, 2006). Other metaphors are context-specific and others are specific to background.

The field of information security is a subset of the information technology industry. As such, there are information security metaphors that share much commonality with the parent industry. There are others that are specific to the field. A recent survey of existing information security metaphors found several common metaphors (Karas, 2008):

- Information Security as Fortress/Castle
- Information Security as Cops and Robbers
- Information Security as Warfare

The same work then explored the overlap of metaphors from the Biological, Medical, and Economic fields as well as the common use of "virtual as physical" extrapolation into what they term the Spatial Domain. After which, the participants of the study created new metaphors. (Karas, 2008) In general, this project was focused on how metaphors facilitated the thinking of threats and solutions. However, many of the brainstormed metaphors serve illustrate how metaphors can break down:

- Cyber Richter Scale – A concept of rating / indexing information technology dangers can help people understand risks, but the existing Richter Magnitude Scale is based on two unambiguous measurements, measurements that do not have an analogous measurement in information security.
- Architecture – The concept of "building in" or "baking in" security works in software / hardware security, but fails in circumstances where something that is already created must be secured. People abandon devastated buildings and throw out bad cakes. Such is seldom an option with compromised servers and networks.
- Wellness – The idea of measuring a system or network on health is a good one. However, one can consider the breakdowns of the wellness metaphor within the existing medical fields to see how it would breakdown within information security. Would treatment be delayed as people run tests? Is there a difference between "colds" that go away and "disease" that must be managed? Should quality of life be discussed?

When working with general or industry-specific metaphors, one must be aware of how far the metaphor extends and what happens when it begins to break down. Advance knowledge of these situations will facilitate communication, particularly in disaster scenarios. Due to this, some people select "favorite" metaphors that they understand and use frequently.

Take, as an example, the results of a metaphor contest run by the author in 2012. The goal was to collect metaphors used within the information security community by members of two communities: the SANS Advisory Board and the PaulDotCom Mailing List. This resulted in numerous security consultants sharing their favorite metaphors. Some, such as these by Michael Smith and Shawna Turner-Rice are fairly general:

Josh More, jmore@starmind.org

"The network is like a castle. To defend the castle you need walls, a moat, archers, guards, a drawbridge, etc. Many castles even have a secret door that is used by the townspeople. They use this to bypass the hassle when they need to go out to work the fields. However, this system only works so long as the townspeople are trustworthy and can be relied on to keep the secret door secret. Skilled attackers ignore all the castle's defense and focus instead on the known weakness. By befriending or posing as a townsperson, they can access the secret door, sneak in, and lower the drawbridge. If a back door exists, it's going to be used. - Michael Smith"

And

"The initial product penetration test is a lot like a person going to the doctor for the first time. There will always be many findings. The difficulty is in identifying which ones are actionable. The younger the person or code happens to be, the more of the findings that will be actionable. This is why security is best considered at the beginning of a project, not the end. -Shawna Turner-Rice"

General metaphors are more accessible by a wider audience. One can presume that the average person will have some level of understanding involving castles and modern medical treatment. They may not be architects or doctors, but there is enough shared context that such metaphors facilitate communication.

Compare those general metaphors to these two examples from Kenton Riley and Jonathan Turner:

Josh More, jmore@starmind.org

"Think of a network like a manned submarine. The submarine is useless without the people inside. It exists to both protect the people from all that water and to get them where they need to go.

- *To reduce the risk of a breach, exterior doors should only be opened under specific situations. New doors should not be added while underwater.*
- *All existing (factory-installed) doors are air-locked with only one door openable at a time, preventing one door failure from causing a breach.*
- *To protect against a breach from harming the people, there are bulkhead doors that can be shut to compartmentalize the damage*
- *Sometimes people go a bit nuts trapped under the water and try to get out. The submarine should do its best to prevent this.*
- *Because of the danger of the water, anything in direct contact with it must be hardened.*
- *Because breaches have happened in the past, all submarines must have a plan for responding to breaching*
- *If a breach does occur, many assessments should be run before re-exposing the submarine to the water.*
- *Just because you're in the submarine and cannot see the water, does not mean that the threat has vanished."*

-Kenton Riley

And

"Security can be compared to football

Josh More, jmore@starmind.org

- *The firewall is your defensive line. It lacks finesse, but will generally stop the big threats.*
- *Other defensive strategies (NIPS, NIDS, etc) are like linebackers. They're there to catch things that get through the defensive line.*
- *Well written code is like cornerbacks. They keep restrict software to the known, safer, paths*
- *Web Application Firewalls (WAFs) are like safeties. They activate when a cornerback needs assistance and helps prevent targeted attacks.*
- *The Security Operations Center (SOC) is like the team of assistant coaches. They keep an overall eye on the details.*
- *The Security Lead is like the Defensive Coordinator. That person collects all the data and makes the strategic decisions around resource usage."*

- Jonathan Turner

These metaphors go much deeper and cover a lot more ground than the more general metaphors. The drawback, of course, is that if person being communicated with does not have an intuitive understanding of football or submarines, the metaphors will fail completely. This is because an understanding of the intricacies of security is now dependent on the understandings of other domains as well.

In short, to be successful, metaphors must be selected in such a way that communication is facilitated between parties and that the introduction of a metaphor reduces rather than increases the complexity of the discussion.

3. Incident Response and Metaphor

During incident management, there is usually a strong focus on the technical. This is not to be avoided. After all, understanding what happened, how to reverse it and how to

prevent it is of critical importance. However, actually implementing an effective defense is often completely dependent on communication skills.

If a defense is going to require new technology, increased budget or control over the way that media covers the issue, communication will be key. At present, the information security industry is young. Lessons in how to frame disasters are known and internalized into the culture of marketing and public relations firms. Lessons in understanding and addressing risks are known and internalized into the culture of financial and insurance firms. Lessons in deploying new technology in a rapid and measurable way are known and internalized into the culture of technological startup firms. In information security, however, we're still learning and our metaphor usage is still relatively ad hoc. Ad hoc metaphors are often used to communicate with outsiders by helping them understand our industry. Little effort is being put forward in how to adapt our understanding to the dominant metaphors of others.

To illustrate the industry's use of metaphor, consider two open source projects and the use of metaphor in their communications.

3.1.Ad Hoc Use of Metaphor by Apache.org

Apache.org is an open source community best known for their stewardship of the Apache web server project. They are well known in the community for having great transparency surrounding the issues they've had. Specifically analyzed will be three incidents covering the years 2009-2012:

3.1.1.2009 – Compromise of apachecon.com

In 2009, there was what is believed to have been privilege escalation attack against apachecon.com. During this attack, the attackers gained full root privileges and were able to hamper investigation. (Apache Infrastructure Team, 2009)

As the response team was writing to a relatively technical audience, the use of technological simplification metaphors is relatively limited. However, the bold note at the top of the report is of particular interest. This sentence is clearly written for a non-technical audience and intended to assuage any readers that the issue was fairly minimal.

> *"NOTE: At no time were any Apache Software Foundation code repositories, downloads, or users put at risk by this intrusion. However, we believe that providing a detailed account of what happened will make the internet a better place, by allowing others to learn from our mistakes." (Apache Infrastructure Team, 2009)*

Note the use of the word "intrusion", though at no point was physical access ever granted to the attackers. This is a common metaphor used within incident response communications and elicits feelings of personal violation. Most intrusions that the average person experiences are relating to their personal space, be it when one child enters another child's room without permission or, as an adult, when a burglar enters their house. This metaphor is, therefore, dependent on the reader/listener having a sense of personal private space. It may not hold up well in cultures that hold property more in common than is typical in Western societies.

The "Internet Attack as Physical Intrusion" metaphor is used also within this report in the phrase "*destroyed* most of the logs". This is intended to indicate a lack of recoverability due to the attacker's actions. However, the common practice of collecting logs off-system would have rendered the "destruction" a mere annoyance. The use of the "network access as physical access metaphor" is used to explain an occurrence, but also to excuse the victim.

When such language is used during an incident, it guides the discussion of the incident. This can help to guide the actions of the organization but in guiding an action, one also avoids actions which conflict with the metaphor in use (Morgan, 2006). This can be critical in a response situation.

Josh More, jmore@starmind.org

3.1.2.2010 – Compromise of JIRA and Confluence

In 2010, Apache.org was attacked through a hosted instance of Atlassian JIRA. This attack resulted in a breach of hashed password data for all users that used JIRA, Bugzilla and Confluence. (Apache Infrastructure Team, 2010)

As before, the richest use of metaphor is at the beginning of the report:

> *"Apache.org services recently suffered a direct, targeted attack against our infrastructure, specifically the server hosting our issue-tracking software." (Apache Infrastructure Team, 2010)*

The use of the word "suffered" is metaphorical, as while the people involved in Apache.org may have suffered during the incident, the services are likely incapable of feeling pain. Similarly, the use of the words "direct, targeted attack" builds upon "suffered" to paint a picture of the Apache organization as a victim being abused. This use of victim language is common within the information security culture. It rides upon a growing push within Western culture to cast victims as blameless and putting focus on attackers as being those responsible. This can be seen in mainstream media coverage of violence (Smith, 2013).

To promote a culture of safety, it benefits a culture to place the expectation of proper behavior on those committing the acts of violence. The use of the language in information security, however, does raise an important question: is it reasonable to expect the same standards of behavior from citizens of a metro area and those of the entire planet? After all, people that live in the same city can generally be presumed to share the majority of a culture's values. Globally speaking, this is clearly not the case.

The appropriation of the "Victim as Blameless" metaphor from interpersonal relations to a global I.T. infrastructure may not be appropriate. Specifically, areas in which this metaphor fails may indicate an overall breakdown of this way of conceiving of and communicating about such issues. Unlike in cases of rape, where there is a growing focus on trying to shift the blame from the victim to the attackers (Smith, 2013), in many

Internet-enabled attacks, the attackers are not known. The societal benefit from shaming the attackers cannot materialize in such a situation, so such a metaphor serves only to excuse poor defense on the part of the attacked businesses.

3.1.3.2012 – Configuration error of audit logging

In 2012, analysis of internal logging server indicated a configuration flaw that could display passwords to interested parties. It is not believed that this data was used nefariously. (Apache Infrastructure Team, 2010)

This incident is of particular technical interest because it concerns a flaw in the implementation of the solution to a reported incident from 2009. Off-system logging was used to prevent the problem that hampered investigation in the 2009 attack. This resulted in a scenario in which logs that contained sensitive data were difficult to purge.

Metaphorically, this report is extremely thin, which is to be expected as there was no damage and, therefore, no need to communicate with an outside group. Metaphor facilitates communication when there are gaps of experience and skill, such as when non-technical individuals such as reporters and CEOs are involved.

When communicating with one's peers, there seems to be an implicit understanding as to when one must use metaphorical and technical language. After all, metaphor can both obscure and clarify and when the risk of confusion by using technical language is sufficiently low as to be expected to not confuse, there is no need to rely upon of metaphors to aid understanding. Therefore, the avoidance of metaphor in such situations can avoid the obfuscation that one's peers might dislike.

This is shown to great effect in the FreeBSD incident report.

3.2.Ad Hoc Use of Metaphor by FreeBSD.org

On November 17th, 2012, FreeBSD experienced a compromise of their development and distribution platform. (FreeBSD Security Officer, 2013)

FreeBSD is an open sourced operating system. To a lay person, this is much like Linux, but to technically-minded individuals, the differences are great. Due to Linux's larger popularity, FreeBSD tends to attract a much more technical user base. As such there tends to be greater commonality between FreeBSD users and the developers of the operating system than there is in the Apache examples. Unsurprisingly, this means that there is much less use of metaphor in the incident report.

The biggest use of metaphor is to distinguish between the "base" and the "packages" for the FreeBSD distribution. While technically metaphorical in nature, this use only facilitates communication with those who have direct experience with the FreeBSD operating system. The overarching intent of the incident report, with its reverse-time structure and heavy technical focus, is to get the reader to understand exactly what the author intends to convey. Compare this to the Apache.org reports where the burden is on the author to understand the limitations of the reader.

Examples of highly technical language which would be completely nonsensical to non-technical users follows:

- *"The Source, Ports and Documentation Subversion repositories have been audited, and we are confident that no changes have been made to them."*
- *"We unfortunately cannot guarantee the integrity of any packages available for installation between 19th September 2012 and 11th November 2012, or of any ports compiled from trees obtained via any means other than through svn.freebsd.org or one of its mirrors."*
- *"We can confirm that the freebsd-update(8) binary upgrade mechanism is unaffected, as it uses an entirely separate infrastructure."*

As with the 2012 Apache report, the use of a completely technical approach can be successful when the shared background between the writer/speaker and the reader/ listener is large and there is little concern about misunderstanding. However, such an approach when there is little shared background could be disastrous, resulting in a

significant amount of time lost in the communication process itself. From an incident management perspective, such an approach should only be considered acceptable if it is guaranteed that no one with a different level of understanding will be involved with the incident in any way.

4. Metaphor Mapping

Ad hoc metaphors will work perfectly fine if the selected metaphors are understandable by those people with whom you are communicating. However, metaphors are constantly shifting and they shape one's thoughts. (Morgan, 2006) Therefore, by choosing to use ad-hoc metaphors, one runs several risks:

- Choosing a metaphor that is nonsensical to the receiver due to a lack of shared experience, resulting in a loss of understanding that must be addressed before communication may resume.
- Choosing a metaphor that overlaps with an ad-hoc metaphor of the receiver, resulting in a misunderstanding that may not be initially detected.
- Choosing a metaphor that conflicts with the ad-hoc metaphors of the receiver, resulting in active resistance to the message being imparted.

Also, if one presumes that the current belief in psychology is correct, that it is easier to change one's mental maps of the world than it is to change the world itself, that people are always communicating, even if not always intentionally communicating and that people are always driven to make the best choice available to them (Andreas & Charles, 1994), then well-selected metaphors will streamline the path to a solution better than many other options.

It may often be wise, then, to put some thought into metaphors before they are used. If approached carefully, this could result in more streamlined communication, faster understanding and less explanation during the immediacy of an incident.

4.1.Analyzing Your Audience

There are many stakeholders in an incident, and the specific groups will vary incident to incident and industry to industry. To streamline the process, consider the eight groups in Forrester's paper "Planning for Failure". (Kindervag & Holland, 2011) Within this paper, Kindervag and Holland reference the following groups that are often affected by failures: All Employees, Information Technology, Corporate Communications, Law Enforcement, Peer Incident Response Teams, Lines of Business, External Business Service Providers, and External Investigators. Using the FreeBSD example of a purely technical incident report, only groups that share sufficient background would be able to communicate. This would likely include only Information Technology and Peer Incident Response Teams. Imagine how much time would be lost trying to explain the situation technically to a group of unskilled employees and law enforcement officials. In situations where time is money, this loss could result in a significant harm to the organization.

Instead of using the metaphors with which one is most comfortable, one should consider using the metaphors that one's audience uses. This means considering their backgrounds and the ways in which they communicate with one another. For the groups listed by Kindervag and Holland, that would likely include:

- All Employees – Little shared background across all departments suggests the use of cultural metaphors. Common experiences that most individuals within a Western culture have in common include going to school (Security as Learning), taking care of family members (Security as Protection), taking care of vehicles/homes (Security as Maintenance) and managing personal finances (Security as Resource Management). Security concepts re-worked to fit into these metaphors will be accepted much more easily than approaching issues from a technical perspective.
- IT – IT groups tend to have significant shared background though not always in the same technologies. Incidents involving a Linux system, for example,

will be much better understood technically in cultures where a majority of the IT staff uses Linux on a daily basis than in traditional "Windows shops". In such groups, it may be wiser to re-craft a metaphor into the dominant technology used. This will avoid discussions around the failure of the metaphor while also avoiding the time loss involved in educating the dominant group about the minority technology. Such metaphors may involve close mappings such as "Remote Code Execution as Leaving Terminal Logged In" or "Denial of Service Attack as Runaway Process".

- Corporate Communications – Corporate communications groups, if they exist, are often well-versed in selecting metaphors for communicating with the masses. Thus, when communicating with these individuals or when communicating with other groups that represent general people outside your organization, such as the Press, it is best to fall back on the most general metaphors as mentioned in All Employees.
- Law Enforcement – Law Enforcement can be a very isolated culture. Unless you are able to deal with a specifically trained group, they must be assumed to be relatively non-technical and focused on Security as Protection, Damage and Capture metaphors. Focusing discussions around what, if anything, was stolen or damaged will lay the groundwork for productive discussion.
- Peer Incident Response Teams – Much as with the Information Technology group listed above, technical discussions will move forward quickly here, as long as there is an overlap in the technical background. If there is not, look for cultural similarities in the areas of detection and response.
- Lines of Business – Different business units also have different areas of focus. The focus will, of course, change with the unit, but stereotypes do work well here. One can generally assume that people in financial business units will respond well to Security as Loss metaphors and that people in service oriented business units will relate to Security as Customer Damage metaphors.

Josh More, jmore@starmind.org

- External Business Service Providers – External providers are often concerned largely with blame. The business model for an external provider is to provide a service at either a higher quality or lower cost than an organization can on its own. In both models, an incident in which the external provider is to blame could risk the business, so there are strong incentives to avoid blame. Metaphors when working with these entities should be based on cooperation and mutual benefit. If this causes a metaphor conflict and the sense that the external provider is not fully communicating, a blame-based metaphor may be used, as long as the blame is not presumed to rest with the provider until all of the supporting information has been gathered.
- External Investigators – Finally, external investigators are much like law enforcement, but may not be as focused on protection and capture as on damage and punishment. These individuals may represent insurance companies, high value clients or auditors determining fines. Metaphors used when communicating with these individuals should be carefully selected to avoid blame, as with providers.

Once you know who your audience is, specific metaphors may be selected to maximize communication.

4.2.Selecting Your Metaphors

Once you have a general set of audience selected, you may begin to fine-tune your metaphor.

4.2.1.Dimension: Industry

Identifying metaphors used within your own industry should be relatively simple. Manufacturing tends to use process or flow-based metaphors. The financial industry uses metaphors around risks and rewards. Other industries describe their work in different terms. Common ways to conceive how organizations work include, machine-based metaphors (process, tasks, precision), organism-based metaphors (growth, death, ecology,

resource competition), brain-based metaphors (learning, self-organization), cultural metaphors (hierarchy, design), and political metaphors (power, goals, individual benefit). (Morgan, 2006)

While this paper is too short to cover as wide a topic as mapping specific metaphors to all industries, a good list of industries may be found online (Bureau of Labor Statistics). Perusing such a list can rapidly provide security insights around metaphorical communication such as:

- Hospitals, Ambulance and Nursing Care Facilities will likely respond better to metaphors that reference risk to patient and patient improvement than to those referring to themselves directly. After all, the people attracted to such roles are often not paid accordingly to the societal value of the services they provide.
- Educational institutions such as schools and colleges are quite similar in that they may be focused on student safety, but also respond significantly to metaphors around learning and general improvement.
- Transportation and Communication industries seem poorly connected to one another, but are both incredibly focused on availability and may not be as concerned about data protection and data loss as other industries.

4.2.2.Dimension: Lifestyle

At a more personal level, metaphors can be selected around societally-common traits such as age and hobbies. This area has been greatly explored in many social engineering resources (Hadnagy & Wilson, 2011), but in general can be summarized as "people understand best what they already know". If you have to regularly communicate complex concepts to a baseball fan, for example, it would be good to learn enough about the game to lay your own metaphors into it. If they are driven by going fishing, cooking or raising their family, metaphors crafted in these areas will be better accepted than trying to get them to see your perspective.

4.3.Metaphors in Incident Handling

Thus far, the discussion has been generally focused on incident communication, but has not specifically called out use of metaphor within the different phases of incident handling. It may be helpful to have a brief overview of how attention to metaphor and communication in general can assist the incident handling process.

4.3.1.Phase 1: Preparation

In the preparation phase of Incident Management, one should consider one's audience. Break the people to whom one may have to communicate with into groups and determine what general metaphors will work best with each group. The goal here is to be relatively complete while recognizing that full coverage will be impossible. The eight items referenced by Kindervag and Holland are a good start, but additional granularity around specific internal business units and key customers or clients might also be wise. This information should be used to create a general metaphor map.

Suppose there is a map of identified groups such that a single metaphor will work for the average person, but not for the executives. For the sake of example, suppose that one of the executives is an avid sports fan and the other grew up on a farm. This is enough data to begin.

4.3.2.Phase 2: Identification

During identification of incident, determine to whom the specific incident is likely to be reported, copy the metaphor map to one used for this specific incident, and update it accordingly. This approach allows the elimination of business units and external agencies that will not be involved in the incident, therefore saving time. The end of this process should include a list of all stakeholders in the incident. This will likely cover system owners, support resources, affected customers, business unit managers and organization ownership. When appropriate, depending on the nature of the incident, each of these individuals should be notified using a mix of technical and metaphorical communication.

Metaphors to be used at this phase could include things like

- General Metaphor –House: We're seeing some sagging in the walls and ceiling. We suspect it might be termites.
- Specific Metaphor – Sports: There are a lot of drug tests coming back as inconclusive. We suspect people might be doping.
- Specific Metaphor – Farming: We're missing a lot of chickens. We need to figure out why.

4.3.3.Phase 3: Containment

Most stakeholders will want to know when the incident is contained, but many will only need to know when the incident has been properly recovered from. Reference the metaphor map being used for this incident and determine which particular phases necessitate notification for each group or individual. Commonly, only technical resources must be notified when containment is complete so as not to mistakenly communicate completion of the incident. For many people, differentiating between Containment, Eradication and Recovery is sufficiently subtle as to take time educating that could be better spent on moving towards recovery. Education of others belongs in the Lessons Learned phase, not in the middle of the process.

- General Metaphor – House: Not applicable. This metaphor would fail if one had to communicate something like "We've trapped the termites in the house!" In this case, failure indicates that the use of the metaphor in this stage of incident handling would be a poor communication decision.
- Specific Metaphor – Sports: We've done the historical research and found a group of people we think are colluding to pass the tests. We are investigating.
- Specific Metaphor – Farming: It's like we've found fox tracks and we think we know how the fox is getting in. We're working on it.

4.3.4.Phase 4: Eradication

Much as with Containment, Eradication communication will likely be technical in nature and updated communication outside of the incident handling team may cost significant time. If, however, certain stakeholders have metaphorical backgrounds that could be leveraged, such updates could be as little as one minute. Compare an explanation of the phases of incident handling to non-technical management with simple phrased updates such as:

- General Metaphor - House: We've killed all the termites, but we haven't yet prevented new ones from getting back in.
- Specific Metaphor – Sports: We've caught everyone we suspected used performance enhancing drugs and they're gone, but we need to review our testing process to make sure it can't happen again.
- Specific Metaphor – Farming: We trapped the fox that was getting our chickens, but we have to fix the coop.

4.3.5.Phase 5: Recovery

Recovery is one of the most important communication stages. This is where the team gets to trumpet success and leave every stakeholder feeling fairly happy about the process. One must convey several things at this stage. First, there must be a general sense of conclusion and that ordinary operations may recommence. Second, if needed, the change in how people have to work must be conveyed as well. Finally, if specific stakeholders are to be invited to the Lessons Learned meeting, that must be mentioned as well.

- General Metaphor - House: The termites are gone; we've replaced all the bad wood and treated around the house. However, we have to re-treat the house twice a year to keep this problem from happening again.
- Specific Metaphor – Sports: We've updated our drug testing system to catch everything we know about and fired the drug tester that was helping people

cheat. However, people are going to keep trying, so we need to periodically review what we're doing to make sure that we can catch them all. I'd like it if you could come to our meeting next Thursday to discuss some specifics.

- Specific Metaphor – Farming: We've filled in the holes in the chicken coop. Interestingly, it looks like the fox first got in when someone left the door open, then chewed his way out. We need to be more careful about that. Could you come to our Thursday meeting so we can review this situation?

4.3.6. Phase 6: Lessons Learned

The final phase of the process is Lessons Learned. This is where the metaphors can start to take a back seat and the team can begin to educate other stakeholders in what happened. This will likely be more technical, but again, the metaphors can be used to streamline things. After the large meeting where the organization discusses the incident itself and how to improve in the future, the team itself should have another meeting discussing how the communication process worked during the incident and how it could be improved. This may result in changes to the base metaphor map.

5. Conclusion

While metaphor has long been seen as a critical tool for creative writers and artists, we all use them. All human languages use metaphor as a core method of communication. Moving from an ad-hoc approach of metaphor to one in which metaphors are custom-crafted to our audience is a very powerful tool for improving understanding.

While improved understanding in and of itself may be a sufficient reason to approach communication in this way improved understanding directly correlates with time savings. This time could be used to resolve incidents. Effectively buying time by front-loading the communication process during the Preparation phase means a faster

path to Containment, which reduces potential damage and a faster path to Recovery, which reduces potential loss of opportunity.

As Benjamin Franklin said, “an Ounce of Prevention is worth a Pound of Cure” (Franklin, 1734/5). Everyone working in Security today knows this. However, our focus on technological prevention may have blinded us to the fact that a successful defense requires a successful recovery. And recovery is driven less by technology than by understanding. We must find ways to drive faster understanding in order to gain faster recovery. Metaphor is one way to do this.

6. References

Andreas, S., & Charles, F. (1994). *Nlp:the new technology of achievement.* New York: HarperCollins Publishers Inc.

Apache Infrastructure Team. (2009, August 28). *apache.org incident report for 8/28/2009.* Retrieved from https://blogs.apache.org/infra/entry/apache_org_downtime_report

Apache Infrastructure Team. (2010, April 09). *Apache.org incident report for 04/09/2010.* Retrieved from https://blogs.apache.org/infra/entry/apache_org_04_09_2010

Apache Infrastructure Team. (2012, May 29). *Apache.org incident report for 05/29/2012.* Retrieved from https://blogs.apache.org/infra/entry/apache_org_incident_report_for

Bureau of Labor Statistics. (n.d.). *Industries in alphabetical order.* Retrieved from http://www.bls.gov/iag/tgs/iag_index_alpha.htm

Dictionary.com. (n.d.). *Metaphor.* Retrieved from http://dictionary.reference.com/browse/

Josh More, jmore@starmind.org

Franklin, B. (1734/5, February 4). *On protection of towns from fire. The Pennsylvania Gazette.* Retrieved from http://www.franklinpapers.org/franklin/framedVolumes.jsp?vol=2&page=012a

FreeBSD Security Officer. (2013, March 23). *Freebsd.org intrusion announced november 17th 2012.* Retrieved from http://www.freebsd.org/news/2012-compromise.html

George, L., Jane, E., Adele, G., & Alan, A. (1991). *Master metaphor list v2.* Informally published manuscript, Cognitive Linguistics Group, University of California at Berkeley, Berkley, CA, Retrieved from http://araw.mede.uic.edu/~alansz/metaphor/METAPHORLIST.pdf

Granneman, S. (2007, February). *Security analogies.* Retrieved from http://www.granneman.com/techinfo/security/securityanalogies/

Gromov, G. (n.d.). *Roads and crossroads of the internet history.* Retrieved from http://www.netvalley.com/cgi-bin/intval/net_history.pl

Hadnagy, C., & Wilson, P. (2011). *Social engineering, the art of human hacking.* Wiley.

Karas, T. H., Moore, J. H., & Parrott, L. K. (2008). *Metaphors for cyber security.* Sandia National Laboratories. Retrieved from http://prod.sandia.gov/techlib/access-control.cgi/2008/085381.pdf

Kindervag, J., & Holland, R. (2011, November 9). *Planning for failure.* Retrieved from http://www.forrester.com/Planning For Failure/fulltext/-/E-RES60564?docid=60564

Josh More, jmore@starmind.org

Kos. (2006, July 02). *Ted stevens on the internets.* Daily Kos. Retrieved from http://www.dailykos.com/story/2006/07/02/224044/-Ted-Stevens-on-the-internets

Lakoff, G., & Johnson, M. (1980). *Metaphors we live by.* (2 ed.). Chicago: The University of Chicago Press.

More, J. (2012, September 12). *[pauldotcom] security metaphor contest - derbycon - winner announced.* Retrieved from http://mail.pauldotcom.com/pipermail/pauldotcom/2012-September/008955.html

Morgan, G. (2006). *Images of organization.* Sage Publications, Inc.

Ortony, A. (1975). *Why metaphors are necessary and not just nice.* Educational Theory, (25), 45-53. Retrieved from http://www.cs.northwestern.edu/~ortony/Andrew_Ortony_files/Why metaphors necessary.pdf

Smith, B. (2013, March 20). *'who is to blame for sexual assault?' the language of rape.* Retrieved from http://www.independent.co.uk/voices/comment/who-is-to-blame-for-sexual-assault-the-language-of-rape-8542165.html

Zhou, D., & Heineken, E. (2009). *The use of metaphors in academic communication: traps or treasures.* Informally published manuscript, Retrieved from http://www.aelfe.org/documents/03_18_Zhou.pdf

Josh More, jmore@starmind.org

Last Updated: December 13th, 2019

Upcoming SANS Penetration Testing

Community SANS Portland SEC542	Portland, OR	Dec 16, 2019 - Dec 21, 2019	Community SANS
SANS Austin Winter 2020	Austin, TX	Jan 06, 2020 - Jan 11, 2020	Live Event
Mentor Session - SEC504	Minneapolis, MN	Jan 08, 2020 - Feb 19, 2020	Mentor
Mentor Session - SEC504	Colorado Springs, CO	Jan 10, 2020 - Jan 31, 2020	Mentor
SANS Threat Hunting & IR Europe Summit & Training 2020	London, United Kingdom	Jan 13, 2020 - Jan 19, 2020	Live Event
SANS Miami 2020	Miami, FL	Jan 13, 2020 - Jan 18, 2020	Live Event
Miami 2020 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	Miami, FL	Jan 13, 2020 - Jan 18, 2020	vLive
Community SANS Columbia SEC542 @UKI	Columbia, MD	Jan 20, 2020 - Jan 25, 2020	Community SANS
SANS Amsterdam January 2020	Amsterdam, Netherlands	Jan 20, 2020 - Jan 25, 2020	Live Event
SANS Anaheim 2020	Anaheim, CA	Jan 20, 2020 - Jan 25, 2020	Live Event
Cyber Threat Intelligence Summit & Training 2020	Arlington, VA	Jan 20, 2020 - Jan 27, 2020	Live Event
Community SANS Quantico SEC504	Quantico, VA	Jan 27, 2020 - Feb 01, 2020	Community SANS
SANS Vienna January 2020	Vienna, Austria	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS Las Vegas 2020	Las Vegas, NV	Jan 27, 2020 - Feb 01, 2020	Live Event
SANS San Francisco East Bay 2020	Emeryville, CA	Jan 27, 2020 - Feb 01, 2020	Live Event
Mentor Session - SEC504	Online, TX	Jan 29, 2020 - Apr 01, 2020	Mentor
SANS Security East 2020	New Orleans, LA	Feb 01, 2020 - Feb 08, 2020	Live Event
Security East 2020 - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	New Orleans, LA	Feb 03, 2020 - Feb 08, 2020	vLive
Community SANS Seattle SEC504	Seattle, WA	Feb 03, 2020 - Feb 08, 2020	Community SANS
Security East 2020 - SEC560: Network Penetration Testing and Ethical Hacking	New Orleans, LA	Feb 03, 2020 - Feb 08, 2020	vLive
Mentor Session - SEC504	Seattle, WA	Feb 04, 2020 - Mar 24, 2020	Mentor
SANS vLive - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling	SEC504 - 202002,	Feb 04, 2020 - Mar 12, 2020	vLive
SANS New York City Winter 2020	New York City, NY	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS London February 2020	London, United Kingdom	Feb 10, 2020 - Feb 15, 2020	Live Event
SANS Northern VA - Fairfax 2020	Fairfax, VA	Feb 10, 2020 - Feb 15, 2020	Live Event
Mentor Session - SEC504	Ann Arbor, MI	Feb 12, 2020 - Apr 22, 2020	Mentor
SANS Dubai February 2020	Dubai, United Arab Emirates	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS San Diego 2020	San Diego, CA	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Brussels February 2020	Brussels, Belgium	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZ	Feb 17, 2020 - Feb 22, 2020	Live Event
Community SANS Omaha SEC504	Omaha, NE	Feb 17, 2020 - Feb 22, 2020	Community SANS