LENS
VENTURES

BRINGING THE FUTURE INTO FOCUS

Encouraging The Uncontrollable

A LENS Executive Summary

Summer 2006

by **TARA LEMMEY**, CEO, LENS Ventures,
and **MOIRA A. GUNN**, Ph.D., CEO, TechNation Media

912 Cole St., #116 San Francisco, CA 94117 888-830-9838

A LENS Executive Summary

Summer 2006

Encouraging The Uncontrollable

by Tara Lemmey and Moira A. Gunn, PhD

In every organization, some things are controllable and others are not. Typically, strategic business analyses seek to control the controllable and make them accountable – in hopes that the impact of the uncontrollable will be minimized.

This is nothing more than wishful thinking.

All executives today – managers, directors, and professional "advice givers" – need to pause and acknowledge what has been happening in all our organizations, well beyond the operational controls so vigilantly put into place.

We have understood for decades that employees act both within and without the official "org chart." So much has been written about it, what more can be said? We all know that Joe in sales gets the scoop from Bill over in finance over lunch. Product designer Mary is influenced by her chats in the coffee line with George from Customer Support. And when there's a real crisis? The Ops Manager might ponder for a moment and then think to call his partner in a foursome from last year's golf outing. Everyone knows that this "phantom" network operates, and that the organization benefits.

So why re-visit it now?

Over the last decade, digital information has flooded every organization from end to end. And while phantom networks have kept on ticking, they now behave very, very differently.

THE "DIGITAL" PHANTOM NETWORK

Corporations today run at breakneck speed … and what might also be termed "breakneck risk." Management registers yet another growth quarter, but is mute about its suspicion that the marketplace is fast becoming saturated. Stock prices remain high, but how much can be attributed to the overheated

procurement of those new acquisitions? And why won't analysts believe that another stable round of profits for this accounting period will continue in the foreseeable future?

On this landscape, the phantom organization is the least of any executive's worries. Yet as a result of the tidal wave of data, this new digital phantom network is already invisibly emerging within his or her organization. And the real news? Intentionally cultivating this network can create a powerful new corporate asset.

WHAT EXACTLY HAS CHANGED? (AND CAN CHANGE EVEN FURTHER)

This past decade has spawned ubiquitous computing and networking, affecting every organization. Still, all organizations are not the same.

What distinguishes one from another is a myriad of factors. How is information created, and who has access to it? Who uses it to create further information, and where can this new data flow? How are decisions made within the organization utilizing that data, and in what ways can the organization respond, given the edge its data provides?

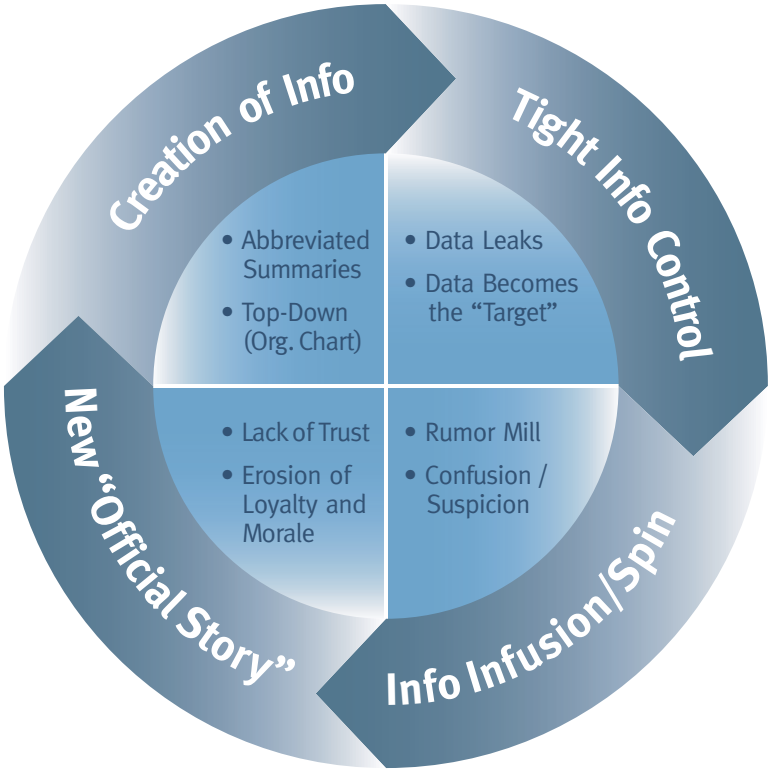
New, forward-thinking organizations spread information far and wide. They also encourage the creation of new information and its dissemination. And they do all this without first knowing if that information is important.

Entrenched, traditional organizations take the opposite, far more familiar, approach. They guard the data carefully, rationing it out to employees on a tightly-controlled basis. Every piece of corporate data is deliberately collected and disseminated at every step of the process.

The difference in corporate culture is concrete and identifiable – the traditional operates on a **"need-to-know"** basis, while the new operates on a **"need-to-share."**

"Need-to-know" organizations are distinguishable in many ways. Data flows down, up, and through the organization according to the official corporate org chart, and it reflects the published and pre-approved group missions. At the expenditure level, more

Control-Based Network
(Need To Know)



resources are spent on data controls then on data infusion, and substantive staff time is dedicated to creating and publishing the official numbers and the official "story," even to employees of that company. The implication is that employees – who share a common corporate goal and can observe the information for themselves – can't or shouldn't figure it out.

To learn about this approach in a post-9/11 government environment, see the work of the Markle task force. ***http://lensventures.com/case_study2.html***

In such an organization, attempting to control all this data – and the data flow itself – is a constant challenge. Information has a way of leaking out, especially to those who love to possess anything they cannot have. One wonders if these workers have the best interests of the organization at heart, echoing the arguments of those who believe widespread data distribution is a bad idea. But seen at another level, this behavior creates the reality. The most closely-held information actually becomes the target. Meanwhile, those with the motivation and capability to act in alignment with the organization's goals and within its value frame continue along, uninformed.

In the “need-to-share” organization, all kinds of data are made available in all kinds of ways. It spreads in an opportunistic way to those who are interested, to those who will – not “can,” but “will” – make use of it. Do you think that Bill only eats lunch with Joe? Or that George only chats up Mary? And yet it was Joe and Mary who took action, both direct and nuanced. They are interested in the data.

Today, the *opportunistic interaction* that breeds phantom organizations goes beyond the water cooler and the “brown bag lunch.” It now also occurs through employee-analyzed, employee-induced information, and this creates the digital phantom network.

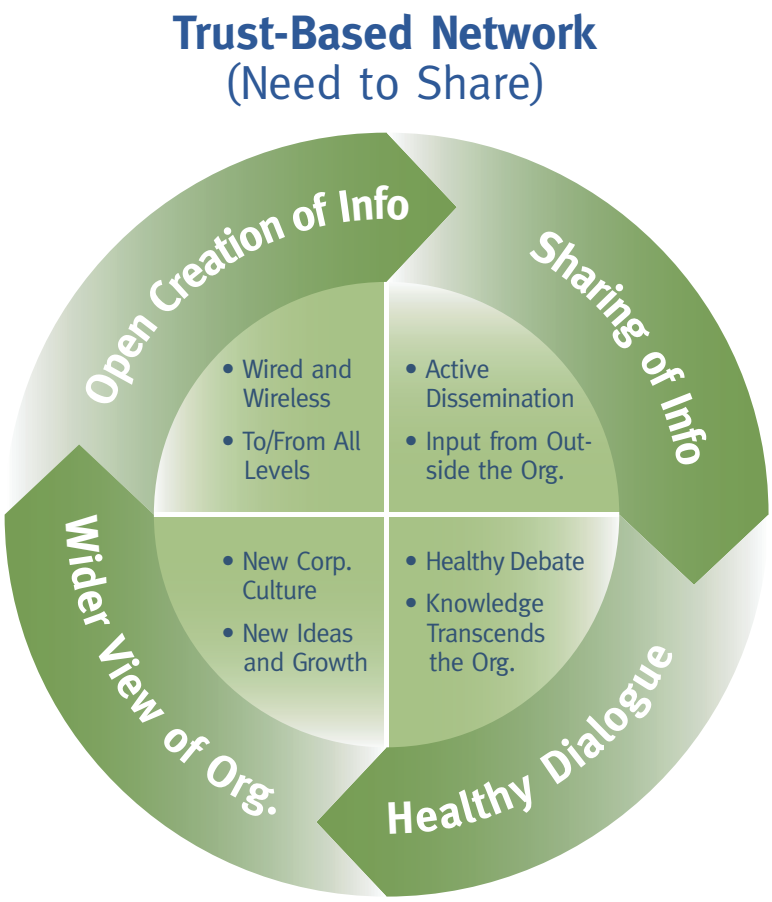
THE DIGITAL PHANTOM NETWORK

Conceptually, the digital phantom network enables connections on a much larger landscape than previously envisioned. Like hallway encounters, annual retreats and staged fruit smoothie socials, its infrastructure has both a physical architecture and a constantly-changing data dynamic. Only now there’s technology.

The hardware itself goes beyond super-mainframes, terabyte storage, desktop computers and workstations, mobile computing, and handheld devices. With data flowing over both wire-intense and wireless connections, also included must be the personal electronics in possession of every employee, including those not provided by the organization.

The data landscape is both familiar and unfamiliar at the same time. Existing conventional data collection and storage continues, but now much of that data is opened up to the organization as a whole. New information sources and source devices are actively sought – email, voicemail, short text messaging, digital pictures, video, impromptu databases to be filled by all comers, and more.

The new phantom-support systems must be prepared to dynamically collect and spread the intelligence of individuals and groups to the corporate knowledge base. Every employee now has a much larger view of the organization. They can suggest new ideas based on personal experience, take confident and innovative action, and contribute back to the corporate body of knowledge.



WHAT DOES A DIGITAL PHANTOM NETWORK BRING TO THE TABLE?

For one thing, a new corporate culture.

Organizations that deliberately develop their corporate infra-structures on a "need-to-share" basis change everything about the corporate culture:

First, there is…

Responsiveness
Customer's needs are not static. Capturing the customer's sensibilities enables the frontline to respond to the customer and feed this information back to the organization. As a result, all manner of products, services and policies can evolve in pace with clients.

This leads to…

Flexibility and Agility

While "responsiveness" measures how well an organization learns from the world around it, "agility" refers to how well the organization can turn that knowledge into action. Both the individual employee and the organization have much more information to work with, including the solutions which others have tried. Simply put, an organization is agile when it has options. To have options, the organization must have knowledge.

This in turn leads to…

Creativity and Innovation

Innovation emerges – not from the head of the solitary genius sitting alone in contemplation, but rather from the sharing of ideas among individuals of like intent. Each sees the world in which they operate as being larger than their single assigned function, and they surround themselves with others who can understand, relate and inform. As a result, many more options come forth. A creative solution is simply one which was previously thought impossible or never thought of at all. True creativity and innovation takes many minds, catalyzed by ever-refreshed information.

With the surprising result that the organization enjoys a new…

Robustness

When there are only a few who make the decisions in an organization or provide input to the leader – so many "more-or-less yes men" in the service of a sole decision maker – it's no wonder that organizations begin to reflect the personality of their leaders, and fall apart when the leader is no more. In the new model, the loss of one essential person – at any point in the organization – does not incapacitate the organization.

This leads to an appreciation of…

Experience & Insight

Once the value of information and true knowledge is realized within an organization, the experience and insight of individuals comes to the fore. Results count, and when informed opinion meets ready challenge, the result is a successful

outcome. Individuals in the organization pay attention to success, and leadership is no longer drawn from lines on the org chart. Leadership is earned and emerges situation by situation.

This is only possible through…

Communication & Social Learning
Within such a system, a premium is placed on the communication between like-minded individuals to share and connect with each other – within a group, laterally across organizational lines, and with groups working on similar problems. There develops an organizational knowledge of group intelligence and available individual expertise.

Which makes possible – and natural – …

Collaboration & Teamwork
Most problems are in some part unanticipated – otherwise they wouldn't be problems. But this also means that the make-up of the most effective team to address any issue cannot be predicted. The dynamic creation of teams – along lines shaped by the problem and the potential solution, as opposed to simply assembling one person from every group or department – is key to success.

Enabling both…

Focus & Complexity
Some problems require focus in a particular specialty and some are highly complex. Solutions are neither easy nor obvious, and time and expertise required to successfully address these challenges cannot be foreseen. The real pay-off comes when teams can undertake dynamically-coordinated and intense tasks without the entropy and apathy that infects complex projects.

Which leads to new modes of…

Leadership & Decision-Making
The level of autonomy afforded a group allows for critical decisions to be made in an informed and responsive manner. Teams can decide on an approach, seek out resources, and coordinate and determine directions without suffering the

delays inherent to a tightly-managed hierarchical system. This process allows for a more experimental approach, fostering creativity and innovation, and relieving the traditional entrenched manager from having to make the "right decision" simply because it's his or her job.

AND YES, THERE ARE APPROPRIATE CONTROLS...

Information which is logically independent of the function of the organization itself, such as salaries, health histories, insurance disclosures, individual financial dealings, etc. must be protected just as it is today. Such data is obviously not appropriate for organization-wide consumption.

It's the operational data that reflects the work of the organization that is at point.

No matter what, all data must travel securely, whether through firewall-protected networks or encrypted public transmission. Dated password schemes for accessing data are being technologically discarded in favor of live biometric and/or voice signatures.

WHAT IF WE BUILD THE NETWORK AND NO ONE COMES?

Perhaps it could happen. But humans aren't like that. They like information. They're innately curious. And in trying to do a job, they frequently want to know anything and everything about it.

To be sure, there will be databases that no one may be interested in, and there may be large portions of popular databases that are never accessed. On the other hand, there may be data which only becomes relevant in a crisis, and that crisis has not happened yet. Data which appears irrelevant one day may be essential the next.

In day-to-day operations, there will certainly be surprises. Digital phantom networks are young yet, and their behavior is evolving. The tools which support and develop such networks are still being created.

In the end, we may find commonality among all organizations … or we may find that each organization is unique, depending on any number of parameters.

But beware …

THE HEISENBERG EFFECT

Once an organization buys into the idea of creating a digitally-enhanced phantom environment, even the "data controllers," who argued against this approach, will begin to salivate. Their suggestions will be as obvious as they are debilitating: Let's track who is accessing what. Let's reward departments that use the data we think they ought to use. Let's acknowledge individuals who are taking advantage of our new system.

This would be a return to the control model, even while we think we're enabling a cutting-edge digital phantom network.

Watch too closely, and we affect the nature and operation of the phantom organization. If we try to capture it – transaction by transaction – the Heisenberg effect comes into play. It will dissolve before our very eyes.

The power of the phantom organization is that it has a knowledge and wisdom beyond the individual and beyond management, and workers must be free to operate within it.

Would you demand that every employee report whom they've made friends with? Had lunch with? A beer after work with? Whom they say hi to in the hallway? Whom they contacted to solve that problem that arose just before the Board meeting?

The temptation to make the phantom organization visible is human, but that destroys its nature. A good organization – a great organization – trusts its phantom structure. It feeds it. Yes, this is an easier thing to do when the stock price is up, and there's nothing in the spin control inbox.

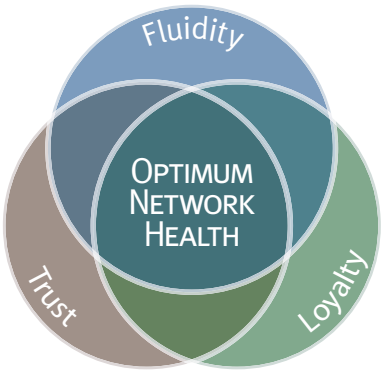
Yet it is entirely possible to determine that the digital phantom network is thriving and benefiting the organization.

DETERMINING THE HEALTH OF A DIGITAL PHANTOM NETWORK

If close examination perturbs the proper functioning of the digital phantom network, how do we know it is being cultivated properly and performing well?

The answer is really quite straightforward: by observing its higher-lever operating characteristics, which, by policy, aren't traced back to individuals, teams and departments; and, very importantly, by observing these characteristics in relation to the human communication backdrop.

The Health of a
Digital Phantom Network



Three core indicators drive optimum network health: fluidity, trust, and loyalty.

Fluidity in organizational structures allows disparate individuals and groups the flexibility to respond in different ways to varied conditions and situations. This is critical in order to mitigate failures in communication, disjointed decision making and inconsistent goals. Fluidity can be promoted by generating multiple paths for data to travel through the network. It is not enough to create the data and provide access; the data must be disseminated and checked throughout the digital terrain. One critical component includes performing real-time audits of data trails, focused more on digital terrain coverage, source and resultant actions, rather than content.

Trust in a network means that members have confidence that trust will be there when it is needed, that available information can be relied upon even when the stakes are high, and that the resources and security of the network can support effective collaboration. Tools can be created to mark the trustworthiness of data. This trustworthiness can be assigned by many parties – the creator, various users, even management. There may also be trustworthiness assigned to users which will and won't permit them to create data, change data and pass trust judgments on data. Trust is earned. It needs to develop dynamically as the network progresses. Tools can include analyzing when a data's trustworthiness unexpectedly declines or is ambiguous. Health means that the digital phantom network is properly policing itself, further guarding against the propagation of misinformation. Lack of health might indicate that the human portion of the network is not engaged.

Loyalty is a worker's positive response to a trustworthy network. It is bi-directional, in that the trust state of the network is in constant engagement with the trust mechanisms of the individual. While not measurable directly, tools which enable reporting of an untrustworthy experience can isolate the response and make it situational. Resolution of these exceptions is high priority for management. An unresponsive incident-reporting system becomes itself untrustworthy. Workers opt out when there is no positive action in response to a trust complaint. This in turn shuts down the worker's willingness to contribute to the system. (Note that this is different from assigning the trust level of data; this is related to the experience of inappropriately assigned trust levels and what the organization does about it from there.)

MITIGATING RISK

While fostering the development of a healthy digital phantom network is paramount, it should not be overlooked that mitigating risk should be an organization-wide goal.

To that end, overtly linking organizational structures – representing both unique expertise and redundant capabilities – can provide a guiding superstructure. This has the further effect of revealing non-obvious sources of expertise and aids in the self-organizing nature of impromptu teams.

WHAT ABOUT PRIVACY AND SECURITY?

Frequently, the first objection to developing these new phantom networks relates to protecting the privacy and security of corporate data. This is no greater a challenge in the face of an active digital phantom network.

Everyone in an organization is governed by a non-disclosure agreement. Everyone is liable to protect the organization. And if they wish to betray it, NDA's, firewalls, and even fanciful encryptions cannot guarantee safety. Any piece of paper can be scanned, any file can be pushed to a flash memory chip which can be pressed into a Treo or a digital camera or into a pocket or a wallet, or transmitted wirelessly. The paths are endless. And easy. And off-the-shelf. And the weak link – or rather the betraying link – is the rogue employee.

And who would argue that the entire data structure of an organization be designed and built to foil the rogue employee? That is the thinking of the "need-to-know" organization. The tail wags the dog.

In the "need-to-share" organization, many are vigilant. Many know who's been regularly accessing what data. Especially newly-created data and data around which there has been a lot of recent activity following a period of no interest. While any worker is free to access data for which his trustworthiness permits, over time "giveaway behaviors," such as shadow-tracing the data of interest to teams in which the worker does not belong, are revealing. Here is another place where the new tools come into play.

DOES THIS CALL FOR A WHOLE NEW DATA ORGANIZATION?

Much of the basic corporate data already exists; the task at hand is to disseminate it throughout the organization. And it's not just final reports. Access to source databases enables others to sift through or otherwise analyze the data. It is here that creative lightning can strike or new insights develop.

For more information on this topic, see ***John Seeley Brown****, www.johnseeleybrown.com*

...and John Hagel's work ***From Push to Pull - Emerging Models for Mobilizing Resources***

New tools are becoming available to support the creation of digital phantom networks, and they are meant to be complementary to in-place systems. Expected functions include pushing newly-created data to the people with whom the creator is in contact in his phantom neighborhood, as well as profiles of the people who the creator thinks should know this information. Collaborative data support includes invitational data bases, sponsored by an individual or group, which asks for data or data leads of interest.

New tools? Yes. A new strategy? Yes. A whole new data organization? No.

NEW ROLE FOR MANAGEMENT? "ENCOURAGE THE UNCONTROLLABLE"

Old corporate environments aren't going to go away in an instant. Let's not forget that for decades, it was believed that

everything an employee needed to know would be given to them by the organization. The corporation knew all, and by default, could control all. But was this ever really best practice? We may well have confused “could” control with “should” control, and encouraged the employee to abdicate personal presence and ownership in the process.

To be fair, this was also a time when it was impossible for an individual at the lowest rungs of an organization to know very much about anything – which is what fueled the traditional phantom organization.

The new role of management is to cultivate the digital phantom network, to ensure its good health and ensure that the employees operate well with this new culture.

Management’s role is to encourage the uncontrollable.

ESSENTIAL ROLE FOR EVERY EMPLOYEE? MAYBE, MAYBE NOT.

While today’s digitally-enhanced phantom organizations are part of the true powerful capability of the corporation, it may not be necessary for everyone to participate. Even today, some people are better “schmoozing” than others. It may prove true, as well, in the new digital landscape.

So the answer is: Sharing data can only be encouraged.

But data unavailable is essentially data nonexistent.

And does this obviate the need for retreats and employee get-togethers? No, a resounding “no.” The organization still runs on people, and at the end of the day, the chemistry between people is not only explicable, but it’s the very magic that make things happen when they need to happen.

It just may be that only a certain percentage of the people in any organization needs to be engaged in the digital phantom network. Only time will tell.

ABOUT THE AUTHORS

TARA LEMMEY is CEO of LENS Ventures, a network of leading thinkers focused on innovation writ-large—from science, technology, and medicine to design, architecture, and sustainability to public policy, law, and economics. LENS Options is their new approach to innovation investment for large firms seeking an easy way to engage in emerging markets. A six-time entrepreneur and technologist, she delights in making the "next" possible.

Ms. Lemmey advises leading-edge companies such as Nokia and Intel on their next-generation strategies and products. She is a member of the blue ribbon Markle Task Force for National Security in the Information Age, where she chairs the Technology Working Group. Ms. Lemmey is a regular commentator in The New York Times, NPR, and CNN on technology, innovation, and the public, as well as a speaker on these issues to audiences such as Future Trends, the Working Women CEOs forum, and the Forbes Top 500 CEO Summit. Her essays have appeared in numerous publications, including The Harvard Business Review, Business 2.0, Internationale Politik, and Wired Digital, and she is a frequent lecturer at universities, including Berkeley, Stanford, and Harvard.

DR. MOIRA GUNN is best known as the host of Tech Nation and its popular segment BioTech Nation, nationally-syndicated on National Public Radio's SIRIUS Satellite Radio Service NPR Now and NPR Talk. Tech Nation also airs on public radio stations nationwide and to 144 countries, and it is a popular podcast via iTunes and the Internet. Dr. Gunn is the Associate Director for Information Systems and Security Programs at the University of San Francisco.

A former NASA scientist and engineer, Dr. Gunn is a member of the Tech Awards Global Leadership Council and remains Board Member Emeritus at the Tech Museum of Innovation. With advanced degrees in Computer Science and Mechanical Engineering, she is also a member of the Dean's Science Advisory Council at Purdue University and the Advisory Board of the Department of Mechanical Engineering at Stanford University. She is at work on her forthcoming book, *"The World We Know Is Changing: What We Can't Control… & What We Can."*