Laugh a Little - It's Good for You

Have you ever laughed so much that your sides ached? It has been established that nothing can make you feel better than a good laugh. Laughter is good for your health. Laughter helps you burn calories, it strengthens your immune system and is able to reduce pain. Therefore laughter really is one of the best medicines you can find.

As a young Work Study Officer I was instructed by my Chief Work Study Officer to read every documents and magazine that were placed on my desk. These magazines included Engineering News; Science Weekly and Medical Weekly. One day I came across an article written about the miracle healing of a terminal cancer patient. The article explained that only having a month to live the man watched all the comedies that he never had time to watch. After a month he returned to the doctor, who was astonished to see the man looking healthy and in great shape. He started questioning him and asked him what he had been doing during the past month. The man explained that he had been watching comedy movies, laughing the month away. The doctor ran tests and found no trace of cancer, thereby attesting that laughter can cure you!

Research has established that:

1. Laughter is like a mini workout.

After a good belly laugh, you may feel slightly out of breath and your pulse would have increased. Laughter may offer the same benefits as a mild workout as it gets your heart pumping and it burns a few calories. According to a study in the *International Journal of Obesity*, you can burn up to 40 calories over 15 minutes of laughter. Even yoga practices laughing as a mild form of exercise with excellent results!

2. Laughter boosts your immunity.
According to the Mayo Clinic, thinking about negative things can cause chemical reactions in the body that can decrease your immunity, however, laughter and happy thoughts have the opposite effect as it releases endorphins (feel-good hormones). These hormones may help reduce stress and boost your immunity. Having a strong immunity will assist you not to get sick that often or to suffer from serious illnesses. Another benefit of feel-good hormones is that they can reduce the feeling of pain.

3. Laughter promotes heart health.
Do you find it funny when a waiter accidentally spills a drink on you? If not, you may be at a greater risk for heart disease. According to research done by the University of Maryland Medical Center, people with heart disease are 40% less likely to laugh in a variety of situations compared to their peers without heart disease. Participants were asked to complete questionnaires and one of the questions were: “If you were eating in a restaurant with some friends and the waiter accidentally spilled a drink on you, would you (a) not find it particularly amusing, (b) be amused but not show it outwardly, (c) smile, (d) laugh, or (e) laugh heartily”. Participants with heart disease were more likely not to find it amusing. To strengthen your heart, it is time to take yourself and life less serious.

4. Laughter improves your mood.

When you are feeling anxious, depressed, or down, you should get some comic relief. A good session of laughter helps relax tense muscles, which is caused by stress and anxiety, and the endorphins instantly changes your mood.

Therefore laughter is good for both the body and soul. So follow the cancer patient example and watch a comedy, or even go to a comedy show or watch one of Trevor Noah's comedy shows, or laugh at yourself once in a while to experience the amazing benefits of laughter.

My youngest son knows exactly how to make me laugh by asking me the following question "What do you call a penguin in the dessert"? Answer: Lost"

THE 'DARK SIDE OF THE NET' ARTICLE SERIES: Second part

Dr Marcus Leaning
Senior Fellow: School of Media and Film
University of Winchester, Winchester, United Kingdom
eMail: marcus.leaning@winchester.ac.uk

and

Udo Richard Averweg
IT Project Manager: Information Management Unit
eThekwini Municipality, Durban, South Africa
eMail: udo.averweg@durban.gov.za

Introduction

This article is the second in a series that considers what we may term the 'dark side of the net'.

Our series looks at a number of practices and activities on the internet that either verge on the illegal or are illegal. Such practices and activities can have serious consequences on how organisations function and we discuss these in the hope that readers may have their awareness and understanding of these issues reinforced. In our first article, published in the December 2016 edition of the Journal of the South African Institute of Management Services, we discussed the activity of spam. In this article we focus our attention on the practices and activities of hacking.

Hacking is a topic that has attracted much attention in the popular press and media in general. Rarely a week goes by without a story appearing of how hackers have attacked a bank or financial institution (Collinson, 2017), stolen money from individuals (Jones, 2017) or even interfered with elections (Gilsinian and Calamuir, 2017). This article considers hacking and looks at some of the reasons people hack and a small sample of some of the more common techniques used. Though hacking is a term of some longevity it has multiple common meanings. The word retains its original Anglo Saxon meaning for chopping wood but in more recent years it has been used to refer to the skilled but unorthodox use of a technology. For example, computer scientists often refer to a hack as a way of circumventing a problem or making a computer system do something that it was not originally designed to do. The term has also been expanded to refer to small techniques used in everyday life to achieve goals (the term life hacking is often used in this regard). Here we limit discussion to the illicit use of or breaking into computers. Such

activity is virtually as old as computers themselves. There is a rich history of examples of attacks upon and through computer systems and we may draw upon an early account to define what we are concerned with. Parker (1976) refers to 'system hackers' and defines the activity they engage in as computer abuse which refers to "any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain". Accordingly here we are concerned with the ways in which computers and computer networks are attacked, penetrated without the sanctioned user's permission or against their interests.

Who are Hackers?

Despite the media stereotype of all hackers being disgruntled youth, there is little that unites hackers beyond their interest in computing. The perpetrators of hacking do not constitute any form of traditional community apart from their interest in the activity itself.

Contemporary hackers come from different societies and countries; have different political persuasions; are of different ages, social classes and educational levels. There is no common value system and notwithstanding the selective cultural construction of the ethical hacker, the understanding of and adherence to appropriate behaviour by hackers is varied to say the least**.**

Why do Hackers Hack?

Given the heterogeneity of hackers it is not surprising that the reasons people engage in hacking are very varied. Here we assert that the reason people hack can be understood in three broad categories. These categories have been derived from reports and accounts of hacking within academic and popular literature (for example, see Décary-Hétu and Dupont (2013), Turgeman Goldschmidt (2005, 2008), Mitnick and Simon (2009)). Furthermore, hackers may well conduct different hacks for different reasons; that is they may hack two organisations for completely different reasons. The three broad categories why people hack are:

- **Economic Reasons for Hacking**

We consider hacking for economic reasons to be those activities that are conducted for financial gain and there are two sub-categories to consider here. First are criminal activities, these are hacks perpetrated to financially enrich the hacker or their organisation. Such activities are increasingly conducted by organised crime syndicates in systematic and complex crimes. The execution of these crimes often utilise other nefarious aspects of the dark net such as spamming and in particular the 'spear fishing' techniques discussed in the previous article in this series and bitcoin or other digital currencies to be explored in our next article. The nature of these crimes are varied but typically involves: stealing money from financial systems such as bank accounts and money transfer systems (Singh, 2015); stealing information either to order (Samani and Paget, 2015) or to sell on data markets (for example, credit card and account holder details stolen from retailers are sold on the dark web (McFarland, Paget and Samani, 2016)), extorting money through the encryption of computers (see the successful attack on Calgary University in 2016, for example (Marotte, 2016)) and threatening to bring down computers using distributed denial of service attacks (for example, Russon (2016) details attacks made on small business in the United Kingdom and South Africa) and data or revealing personal and incriminating information (O'Neil, 2016)). In addition to the hacking of computers for nefarious purposes there are also numerous companies that offer the service of penetration testing; they attempt to break into computer systems to test the security systems in place for a fee;

- **Political Reasons for Hacking**

The second category relates to what we may term political reasons for hacking. Here there are two further subdivisions. First are those who hack so as to seek redress for what they perceive to be a political injustice. These groups deploy hacking skills to further the political aims of particular groups or political parties or to challenge and damage other political groups, agencies and governments. Such groups often operate under the portmanteau of 'hacktivist' – an activist who hacks. A contemporary example of such a group would be the hackers collective Anonymous which has attacked various targets it perceives as being oppositional to it political stance. Anonymous emerged out of the Occupy movement and shares many of the political concerns as Occupy (Goode, 2015). Second are those who hack on behalf of a government against either domestic or foreign targets. Examples of this include governments attacking foreign companies such as North Korea attacking Sony in revenge for releasing the film 'The Interview' – a satirical film about a planned assignation of North Korean Supreme Leader Kim Jong-Un (Sherr and Rosenblatt, 2014) and Israel's involvement in developing the Stuxnet virus that was used to disable a nuclear reactor in Iran (Lindsay, 2013); and

- **Personal and Social Reasons for Hacking**

The third main reasons for hacking may be considered social reasons. These relate to an individual's personal circumstances, beliefs and interests. We may sub-divide the category into three sub-divisions: the first relates to personal interests and includes reasons such as mischief, the desire to vandalise websites for pleasure, the thrill of trespassing in systems without permission and receiving the fame and reputation amongst peers (Taylor, 1999). The second sub-division relates to individuals seeking redress against others for perceived slights. Here attention turns to inflicting cyber-mediated harm to another. There have been numerous conflicts between hackers and the authority within groups which is enforced through hackers attacking each other and 'doxing' (obtaining and releasing personal information about someone) (Sammons and Cross, 2016). The third sub-division concerns disgruntled employees who seek redress for a perceived work based grievance. Such 'inside jobs' pose a serious problem for organisations as the attacks subvert the defences developed to counter normal externally originating attacks. Furthermore in certain instances it is the very people who are responsible for establishing and maintaining the defences who commit the attacks.

Common Methods of Attack

In this section we move to discussing some common hacking attacks and practices targeted at individual users of computers. These techniques are used by hackers to gain entry to computer systems and once in, they can conduct the more advanced activities such as stealing data and using the compromised systems as stepping stones to other targets.

There are a vast number of techniques and new ones are continually developed and invented. Moreover, some of the techniques are significantly technical in nature and a meaningful discussion would require expansive descriptions of how certain aspects of internet communication operates. For example, a hacker who goes by Anonymous Africa, in June 2016 attacked a number of the public broadcaster's (South African Broadcasting Corporation (SABC)) websites and 'knocked them' offline (Vermeulen, 2016). The hacker was asked how he 'took down' the SABC's websites and responded with "DNS reflection. Lots and lots and lots and lots of DNS reflection" – clearly with such a technical response, one would need to understand the internet service that translates domain names into internet protocol addresses – the Domain Name System/Service/Server (DNS).

In consequence our discussion focusses on a selection of nine common techniques of hacking attacks and practices. We limit the discussion to a more general description of each:

- **Distributed Denial of Service**

The Distributed Denial of Service (DDoS) is a common attack used to slow down and crash websites and web services. It involves bombarding a web server with multiple requests simultaneously to the point at which the server is unable to process the requests and slows down and crashes. This is commonly performed by using multiple computers which at a given moment start to send requests to the server. Typically the computers used are not the hackers' computers but are those which the hacker has taken over and then recruited to their 'bot net' or zombie army. The bot net computers are recruited through the spread of viruses through emails as discussed in the previous article in this series. Once recruited the infected computer can be instructed to participate in the DDoS at given times. Typically the compromised computer is not disabled entirely and still functions most of the time so as to not alert the user to its infection. DDoS are used in a number of different ways. They can be used simply to attack and take down a site; they are used to disable a site so that other forms of compromise can then be conducted; and they are used to extort organisations and individuals where the target organisation is threatened that unless they pay, a few of their services will be attacked;

- **Keylogging**

This is another piece of code that is distributed by spam email. Moreover it often has no other impact upon the computer it has infected and resides on the computer surreptitiously; it also often infects computers in cyber cafes and other public access points. The keylogger software simply records all keystrokes entered on a keyboard during a session. The information is then sent to the hacker's computer where other software looks for website names, user names and the follow up password in the text file - thus revealing when a user logs into a particular web service such as an online bank account, PayPal account or email service**;**

- **Click Jack Attacks**

A click jack attacks uses an invisible top layer to a website which the user clicks or enters information. In this way the hacker can have the user perform actions on their computer which will afford them other opportunities to attack or record information while the user believes they are entering into the genuine webpage**;**

- **Wireless Access Attacks**

Wireless networking affords hackers multiple means by which they can attack users and consequently organisations. Hackers may monitor traffic sent by wireless means. While some of this will be encrypted there will be some that is not and this allows the hacker to obtain information. Hackers can also establish their own free wifi systems allowing free access to the internet, however, all data sent through these systems can be monitored and used (if not encrypted);

- **Fake Websites**

Websites that replicate genuine bank and other services are established by the hacker. Typically these sites are hosted on other unsuspecting users' computers. The sites appear genuine and include all the graphics and features of the target site. Once the user has keyed in their user name and password, the information is sent to the hacker and the user is redirected to a page that indicates their password is incorrect and is asked to re-enter it. This time, however, the user is sent to the genuine site and often assumes they

entered it incorrectly the first time. Users are often driven to the fake sites through phishing emails sent to them requesting they log into their accounts;

- **Fake Programmes and Applications**

Here the hacker has produced computer programmes and applications (commonly referred to as 'apps') that look or sound like genuine apps. Once the user downloads and runs the imposter, the programme or app performs other actions than those the user intended**;**

- **Backdoors in Legitimate Programmes**

A number of commercial programmes have 'backdoors' that allow computer engineers to perform actions for the purposes of service; when hackers become aware of such 'backdoors' they can use them to access the host computer;

- **Cookie Capture**

Cookies retain data input into web browsers to assist the web developer and save the user. Hackers can remotely steal this information and therefore avail themselves of the information retained in the cookie; and

- **Ransomware**

Ransomware is software that encrypts certain files on a host computer and requires the user to pay a fee for the key to unencrypt the information.

Concluding Remarks

In the internet's dark economy, cyber security is the most important form of security that all organisations must be concerned with. Since organisations organise and store their information electronically, such information may easily become vulnerable to malevolent computer hackers. Such hacking activities can have serious negative and dark consequences for organisations. In our third article in this series on the 'dark side of the net', we discuss the activities of crypto currencies and bitcoins.

Further Reading

Collinson, P. (2017, 23 January 2017). Lloyds bank accounts targeted in huge cybercrime attack. The Guardian, Retrieved from: https://www.theguardian.com/business/2017/jan/23/lloyds-bank-accounts-targeted-cybercrime-attack

Décary-Hétu, D. and Dupont, B. (2013). Reputation in a dark network of online criminals. Global Crime, 14(2-3), 175-196.

Gilsinian, K. and Calamuir, K. (2017, 6 January 2017). Did Putin Direct Russian Hacking? And Other Big Questions. The Atlantic.

Goode, L. (2015). Anonymous and the Political Ethos of Hacktivism. Popular Communication, 13(1), 74-86.

Jones, R. (2017, 14 January 2017). 'I thought I'd bought my first home, but I lost £67,000 in a conveyancing scam'. The Guardian. Retrieved from: https://www.theguardian.com/money/2017/jan/14/lost-67000-conveyancing-scam-friday-afternoon-fraud-legal-sector-email-hacker

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3), 365 404.

Marotte, B. (2016). Digital hostage. The Globe and Mail. Retrieved from: http://www.theglobeandmail.com/news/national/how-the-university-of-calgary-hack-wentdown/article30358657/

McFarland, C., Paget, R. and Samani, F. (2016). The hidden data economy. Mcaffee report. Intel Security.
Mitnick, K. D. and Simon, W. L. (2009). The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers: Wiley.
O'Neil, S. (2016, 27 October 2016). The Skype sex scam - a fortune built on shame. Retrieved on 10 February 2017, from http://www.bbc.co.uk/news/magazine-37735369
Parker, D. B. (1976). Crime by computer. Scribner, NY, New York, USA.
Russon, M. A. (2016). 'Armada Collective' hackers to launch bitcoin-extorting DDoS attacks on unwitting victims. International Business Times. Retrieved on 10 February 2017, from: http://www.ibtimes.co.uk/armada-collective-hackers-launch-bitcoin-extorting-ddos-attacks-unwitting-victims-1579789
Samani, R. and Paget, F. (2015). Cybercrime exposed: Cybercrime-as-a-service. Corporate white paper, Santa Clara, Calif.: McAfee Labs, 2013a. As of September, 29.
Sammons, J. and Cross, M. (2016). The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy: Elsevier Science.
Sherr, I. and Rosenblatt, S. (2014). Sony and the rise of state-sponsored hacking. CNET. Retrieved on 10 February 2014, from: https://www.cnet.com/uk/news/sony-and-the-rise-of-state-sponsored-hacking/
Singh, N. (2015). Online frauds in banks with phishing. The Journal of Internet Banking and Commerce, 2007.
Taylor, P. A. (1999). Hackers: Crime in the Digital Sublime: Routledge.
Turgeman-Goldschmidt, O. (2005). Hackers' accounts: Hacking as a social entertainment. Social Science Computer Review, 23(1), 8-23.
Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. International Journal of Cyber Criminology, 2(2), 382.
Vermeulen, J. (2016, 13 June 2016). 'This is how I took down the SABC: Anonymous hacker'. Mybroadband. Retrieved on 13 February 2017, from: https://mybroadband.co.za/news/security/168303-this-is-how-i-took-down-the-sabc-anonymous-hacker.html

HR Standards

By Marietjie Lotz

Overview

The so called “poor” quality service experienced in South Africa is nothing new and certainly not confined to South Africa. In fact, it is a worldwide phenomenon. And when you ask those who complain about “poor” quality, you soon learn that just like beauty, what is defined as “poor”, differs according to individual expectations; and this can be directly attributed to the fact that there are no clear standards according to which the man in the street can expect to be served. Whether the root cause can be attributed to differing expectations or a lack of respect towards citizens, the bottom line is, to define something as poor, one must have a clearly defined and measurable standard to compare the quality to.

The concept of quality service has prompted many students of human behaviour and industrial psychology to attempt to unravel the Holy Grail that might provide the formula for a magical turnaround in productivity and the quality of service or products to satisfy human kind for a few more millennia. As a result the correlation between Human Resource Management (HRM) and organisational performance has been studied comprehensively in order to dichotomize the information available about “best practice concepts” or “universal set of best HRM practices for the best fit” etcetera. And in spite of all that have been discovered, there still is no guarantee that if you revolutionise all the HR management policies, practices and rules, you will have an effective organisation that would meet 100% of the public expectations 100% of the time. That is why clear standards for service delivery have become such an important component of service delivery worldwide. Wastage cost money and the entire world economy is feeling the squeeze of increasing unemployment, consistent job shedding, rising security threats and a decrease in per-capita spending flagging that the economy is actively deteriorating on many fronts and that requires drastic reforms to turn the situation around.

Development of Standards

As stated by Wikipedia, the use of standards assists in the creation of products and services that are safe, reliable and of good quality. The need for service standards gave birth to the International Organization for Standardization (ISO) standards which are voluntarily followed by many countries all over the world. ISO affirms that the application of standards guides the increase of productivity while also minimising errors and wastage. Standards is one of the instruments which is used to develop sustainable and competitive global trade on a fair basis, while it serves to safeguard consumers and end-users against exploitation and ensures that products and services conform to the minimum requirements. The same goes for Government and non-governmental services of the non-profit kind. They too have a legal and moral responsibility to deliver a service fit for purpose to the public.

Performance

Nowadays, organisations develop performance plans, whereby they establish performance goals that are objective and measurable, they determine performance indicators to measure outputs. There are service level agreements and predicted outcomes for each programme and they submit performance reports as prescribed by their respective industries and yet, if one opens a newspaper or switch on the radio, there is someone reporting about a protest somewhere in the country concerning a lack of service delivery.

The questions that beg to be answered are: Where does the disconnection between the expectations and the actual delivery come from? Why are the performance expectations of the public still not met, after multiple stakeholder consultations, clear visions established, missions determined, plans developed, performance indicators identified and standards and measurements developed to support service delivery? Why does the "system" not produce the required results?

Planning, strategising and monitoring are expensive tools of the trade. It swallows a huge portion of human capital and financial resources from the budget, yet the return on this investment continuously presents itself in public outcries, protest action and in worst case scenario, sometimes the death of the most vulnerable of all.

Role of HRM

Many researchers argue that for HRM to be successful, it should be embedded in the strategic needs of the organisation. This means that there should be a vertical alignment between the HRM strategy and the business goals to support and reinforce the business objectives in order to be a significant strategic driver of productivity from inside the organisation. Gone are the days for HR to be the fashion police of the organisation. Gone are the days of HR's role to being restricted to that of an "administrator" or "support function".

This practice is just too costly for any organisation to accommodate in this day and age. HR's role must encompass amongst others, that of an enabler of service delivery according to a predetermined standard. The HR manager should understand the key value-adding activities of the organisation and how standards could improve the implementation of policies and practices in order to facilitate service delivery. He or she should be a master strategist, an expert analyst, planner and driver of implementation. How do you recruit, employ and monitor performance, if there are no clearly defined service standards for each business process to compare individual and organisational performance against? Is our current performance management system a reliable tool for measuring performance? Do we still measure output instead of outcome and what is the difference between these two concepts in productivity terms? What exactly is missing from the service delivery value chain to make the system work?

HR Standards

Edwards Deming set out to define management standards for routine processes for as many functions in an organisation as possible. His vision was that if the routine is followed consistently a predictable result should follow. The actual result could then be compared to the expected result which would then be a reliable indicator of the level of achievement, and as a result, service standards for HR practices were born to inspire, educate and support managers and employees with regard to the fundamental role of HR in creating an effective organisation.

The SA Public Service Context

The transformation that was envisaged in 1994 through the White Paper on Human Resource Management in the Public Service where the focus was shifted to service delivery outcomes instead of inputs was found not to produce the required results. The White Paper on Transforming Public Service Delivery (WPTPSD) of 1997, commonly known as the Batho Pele policy was aimed at redressing the way public services were rendered. The Batho Pele principles provided a framework on how public services should be provided for improving the efficiency and effectiveness thereof. From the literature review, it was evident that improved public service delivery depends on several aspects ranging from Human Resource Development (HRD) to performance measurement and

accountability. The need for improving efficiency and effectiveness of the Public Service was emphasised throughout the various pieces of legislation. It was evident that these principles should be incorporated in the performance contracts of all employees so that performance could be assessed against them and ultimately improve service delivery.

Government defined the said principles to form the basis of the early service delivery planning value chain, yet, the paradigm shift envisaged in service delivery did not follow the natural maturity of the belief set and because this approach requires the involvement of the public in holding the Public Service accountable for the quality of service provided, members of the public felt that they have the right to demonstrate their dissatisfaction in various tangible ways.

Meanwhile employees were required to sign performance agreements as part of their employment contracts, they developed annual performance plans; their performance was measured trough the analyses of volumes of data and annual reports that were published as part of the accountability loop of good corporate governance, without logically connecting the parts of the overall system. Continuous performance and compliance audits are still conducted throughout the expenditure framework life cycle and the Auditor General and Parliament hold Executives accountable for every little detail connected to the performance of their respective organisations, yet very few Departments have service delivery improvement plans in place, while the improvement of services to the public remains slow.

There is thus an important knowledge management aspect for the implementation of standards, in that the process makes implicit knowledge explicit, shared and replicable. HR Management has been a function largely ignored by quality assurance experts, possibly because it deals with the so-called “soft” issues of human behaviour. However, after decades of academic research into the function, it is possible to state with confidence that if certain processes are followed, certain outcomes will result. So for example, if employees are kept informed on how their work links to the strategic objectives of the organisation and are also kept informed on how well they are performing their own work against the standards expected by the organisation, we can predict, based on empirical research, that employees will be better motivated to perform well and will feel more satisfaction in their jobs and more engaged with the organisation.

In South Africa, many aspects of HR management are regulated through labour legislation, amplified by the Codes of Good Practice issued by the Department of Labour. There are a plethora of legislation that HR managers must ensure compliance with. However, this comprehensive set of legislation and Codes does not provide a useful management model for HR work and thus HR work differs considerably between organisations. An HR professional moving jobs has a great deal of familiarisation to do with “how HR is done around here”. This lack of an HR management model has contributed to the lack of standing of HR as a profession compared to other professions and functions and HR practitioners does not have an accepted “tool box” to improve the functioning of the organisation, making it much more difficult to persuade executives and line managers that the introduction of certain HR practices is a good idea. HR Management has been a function largely ignored by quality assurance experts, possibly because it deals with the so-called “soft” issues of human behaviour. However, after decades of academic research into the function, it is possible to state with confidence that if certain processes are followed, certain outcomes will result.

Currently, there are no accepted management standards for HR management, although some elements of the European Foundation for Quality Management (EFQM) Excellence

model clearly refer to concepts within the HR field of expertise. The Investors in People (IiP) standards are aimed at ensuring improved organisational performance through better people processes, but the scope of the IiP standards are not comprehensive in terms of HR Management. ISO is working on some HR standards, but progress is slow and publication is not expected for some considerable time. The Society for HR Management in the US (SHRM) has approached the problem of the lack of standards from the investors point of view, reasoning that if investors can be presented with statistics or metrics which have been prepared on definitions used on a standard basis by organisations, the investors will have the basis on which to perform comparisons between companies and thus make better investment decisions. The good news about this approach is the recognition that HR processes can make a difference to the value of a company in that the outcome of those processes can be measured by the standard metrics and evaluated by investors

In other words, there is a very clear accountability basis for service delivery, however, the "how" part of service delivery improvement remains unclear. In order to address the "how" part, the DPSA has developed a framework or tool kit that involves:

1. Business Process Mapping, review and management
2. Standard Operating Procedures
3. Setting of Service Standards, and
4. Service delivery improvement plans

These fundamental processes forms part of the systemic approach that aims at harnessing the collective knowledge available to raise efficiency and effectiveness levels.

The value chain consists of the following eight steps:
1. Strategic Planning
2. Develop service delivery model
3. Business process management
4. Standard operating procedures
5. Unit costing
6. Service standards
7. Service charters
8. Service delivery improvement plan

To ensure that human resource management in Government make a difference, there must be visible uniform standards for HR practices throughout the different Government Departments and the three tiers of Government. These practices require committed execution and compliance by all line function managers because ultimately, they are the ones managing their own human resources. The best human resource strategies, policies and practices are doomed for failure if it is not implemented consistently, ethically and effectively across the organisation by all the line function managers.

In line with outcome 12 of the Delivery Agreement of the President of South Africa, the DPSA was tasked to lead the approach towards the development of norms and standards for the entire Public Service. Subsequently Departments were tasked to use Business Process Mapping and the development of standard operating procedures as a precursor for setting measurable service standards for all the value chains in their Departments and to develop service delivery improvement plans for the outer years of the implementation cycle.

Conclusion

The purpose of this article was to highlight that the challenge of ineffective service delivery is a universal/ world-wide challenge and not only a South African phenomenon. It was emphasised how the expectations of the public can differ vastly from what is realistically achievable within a constrained economy. As was captured in one of the earlier state of the nation addresses, "A transformed South African Public Service will be judged above all by one criterion: its effectiveness in delivering services which meet the basic needs of all South African citizens." Improving service delivery is imbedded as the ultimate goal of the public service transformation programme since 1994. The Batho Pele White Paper states it clearly: "public services are not a privilege in a civilised and democratic society: they are a legitimate expectation".

The article further highlights the importance of communication and consultation when setting service standards and how the Batho Pele principles became a major driver of service delivery improvement in the Public Service. It was also emphasised how important it is that all HR polies and practices support the organisational vision, mission and strategy and how HR policies and labour legislation, recruiting the right people to do the job, managing these people and their performance, developing their skills and executing effective HR planning, forms an integral part of the job of the line function manager. Managing human resources are no longer the responsibility of the HR manager alone, but it has become everyone's business.

As captured on page 10 of the conclusion of the DPSA Toolkit on Service Standards – October 2011, "service standards should be simple to understand, relevant and meaningful to the user and the recipient of the service." This means that they must cover the aspects of service which matters the most to the recipients of the service.

"Some standards will cover process, such as the length of time taken to authorize a housing claim, to issue a passport or identity document, or answer a letter. Other standards will be about outcomes. In the health arena for example, standards might be set for the maximum time a patient should wait at a primary health care clinic, or for a non-urgent operation... This means that they should reflect a level of service which is higher than what is currently offered, but what can be achieved when a dedicated effort is made..."

According to a Public Service Commission report, Departments develop service standards in order to do away with ambiguity and thereby ensure that citizens have realistic expectations about the nature of the services being delivered. Service standards also promote a culture of effectiveness and efficiency, as they are typically used by managers in a department to measure the performance of that department. Importantly within the South African context, service standards promote accountability and transparency, as standards represent a public commitment by a department that they will deliver services that meet the needs of the public in the most efficient and effective manner.

It is further stated in the report that improving service delivery is a continuous process for departments and not a once-off task. It calls for a shift from inward-looking bureaucratic systems, processes and attitudes to searching for new ways of working that will give priority to the needs of the client. The government of South Africa is committed to modernising public service management processes and improving citizen satisfaction with the services it delivers

The article also touched on the role of the South African Board for People Practices (SABPP) that has done a lot of work on the development of an HR management model for South African conditions. This model is based on strategic, functional/operational and performance measurement, which is also linked to the classic quality assurance framework of prepare, implement, review and improve. Researchers then used this information to develop the national HR Competency Model which deals with leadership and personal credibility, organisational capability, solution creation and implementation, interpersonal and communication skills and citizenship for the future. This model clarifies the professional skills required to be a successful HR practitioner in today's fast changing work environment. This model also provides a foundation for the continuous professional development of HR professionals.

Globalisation has ushered in a new era of complexity, uncertainty and change in all sectors. The competition for scarce resources is growing continuously. The new generation employees are no longer satisfied to work in a rule driven inflexible work environment. They want to maintain a certain level of freedom, creativity and flexibility. That is why performance agreements and service delivery standards must be clarified right from the recruitment stage, in order to ensure that the right person is appointed in the right position.

The same goes for servicing the expectations of the recipients of services. They want to know exactly what they can expect, by when and how, and that is why customer needs are identified as the underlying force that will have the biggest impact on an organisation's talent requirement in the years ahead. As emerging markets are becoming the new centres of gravity for the global economy and the top strategic priority, competition for talent is becoming fiercer.
Finally, service standards reflect positively on the image of an organisation, both with employees and the public at large. By illustrating an open approach to what the client can expect as a standard of service, it creates trust and has a positive psychological influence on customer satisfaction.

Bibliography
Operations Management Framework - May 2015 (2).
DPSA Toolkit on Service Standards March 2013
SABPP National HRM System Model and Standard August 2013

THE FIVE HIDDEN WASTES

Based on Ron Crabtree's report
5 Hidden Profit –Sapping Wastes (published 2011)

The development of standards are supposed to assist organisations with improved productivity but as we all know organisations are riddled with waste which has seen the development of the 5 s's which are: Sort, Systemise, Sanitise, Standardise and Sustain. The 5's are part of Lean Management Tools whereby an organised workplace reduces wasted time and a clean workplace reveals problems. But organisational waste is not only in physical form it is also manifested in the organisational culture and personal productivity and these wastes also have an effect on productivity and service delivery.

What are organisational wastes? Resources consumed by inefficient or non-essential activities.

Wastes are any efforts that don't directly add value and we have to earn our pay by providing more value to our customers than what it costs to produce our services and products (principles of Batho Pele, value for money).

The five hidden wastes are:
1. Internal communication breakdowns
2. Poor personal productivity and time management
3. Ineffective meetings (not enough or too many)
4. Knowledge disconnection
5. Lack of organizational focus on "value add"

1. Internal communication breakdowns

Here are some examples related to the above:

- Chasing after people for approvals;
- Searching for resources or information;
- Inconsistent or incomplete requests;
- Missing information or empty spaces on forms;
- Reprioritization waste- which leads to interrupting lower-priority tasks to assist activities which are in crisis;
- Excessive work in process/lack of organisation and prioritisation;
- Searching or looking for materials due to ineffective computer tools.

2. Poor personal productivity and time management

Experts argue that 20% of the time you spend at work each day accounts for 80% of the value you create. In most service industries this is more than likely true for many of the workforce and in particular for middle managers and above. These employees struggle, to a greater or lesser degree, with massive amounts of hidden waste and this leads to losses in their personal productivity, leading to them never having enough time to do things right. They feel stressed when they have to find information they need to complete a work assignment. They have to deal with many interruptions every day. Forcing them to multitask in order to survive and not to fall behind and unable to focus on priorities due to someone else's poor planning or in some cases- urgent ad-hoc works instructions.

3. Ineffective meetings (not enough/too many)

Most organisations generally have ineffective meetings, or they have either too many or not nearly enough meetings. Very few organisations get it right on a consistent basis. This is particularly true in service operations.

Signs of ineffective meetings:

- People feel that at least 80% of their time is wasted.
- Meetings don't produce clear "next step" actions and accountabilities for actions on a timeline.
- People come late or are unprepared or they take meetings over with their own agendas.
- Attendees display dysfunctional "anti-team" behaviour.

Signs of too many meetings:

- It takes an administrative assistant an hour to schedule a meeting with more than three people, even with an automated scheduling system, because the people are already booked solid for several weeks.
- Every board room in the building is already booked for the next week, making it

impossible to schedule a meeting.
- People spend so much time in meetings that they have to come in early or stay late to get their “real work” done;

Signs of not enough meetings:
- People feel uninformed about what’s going on.
- Decisions are made that conflict with other parts of the organisation due to a lack of coordination between people.
- Problems faced by the business take a long time to solve because the staff doesn’t discuss them often enough or in a structured forum.

4. Knowledge Disconnection

The term knowledge disconnection means, "a failure to truly know what customers want from us." This concept includes “internal and external customers. Your internal customers are those employees who depends on someone else to do something before they can do their jobs. The theory is - if you fail to treat each internal process customer with the same concern you have for the external customer, you will end up underperforming. Because business processes deliver results. The ability to deliver a desired result is by the weakest link in the chain of processes that ultimately deliver to the external customer. These processes are performed by internal customers. Everything in an organisation is in fact affected by everything else. By focusing on your internal customers, you will be optimizing your part of the value chain in the organisation.

5. Lack of organisational focus on “value add”

Many times people are caught up in doing things because it seems like the right thing to do. There can be easy confusion between an activity and adding value or not become confused with “busy” versus “productive**.”** Therefore it is a challenge to make sure that activities performed in the organisation delivers value to the external customers, directly and indirectly, through the internal process customers.

What are the value-add tasks:

Working directly with a customer or converting information into a form that someone else needs to do the next value-add step in the process.

An activity qualifies as a value-add step when:
- A physical transformation occurs – There’s a change in the shape of form of a product, a service, or information.
- It’s done right – The activity isn’t some form of reworking, inspecting, double-checking, just-in-case copying etc. A step should be done once, correctly, and it should NOT require verification or duplication later**.**
- A customer wants to pay for it – If a customer doesn’t care about the activity strongly enough to literally pay for it on a detailed invoice, it’s NOT a value-add step.

Outright waste – A non-value-add (NVA) activity
- Business-necessary waste – Business-necessary non-value-add (BNVA) activity, or necessary but non-value-add (NNVA) waste (you pick the term you like best)
- The NVA steps are called “low-hanging fruit” opportunities that you can deal with sooner rather than later. Many of these can be addressed with better work design or changing policies that inadvertently drive waste.

You can use brainstorming techniques to identify where the waste in your organisation by visiting www.OperationalExcellenceEdge.com. There is a step by step guide on how to conduct sessions with staff to determine waste areas.

Bibliography: report by Ron Crabtree and MetaOps Inc., publisher of Operational Excellence Edge: No More Wasted Time, Money and Resources.
Read more: http://www.businessdictionary.com/definition/waste.