# Password Psychology in the Age of Cyber Pirating

**By Leandri Lotz**

How to safeguard your personal information against prying eyes.
Password
Noun

- A secret word or phrase that must be used to gain admission to a place.
- A string of characters that allows access to a computer or service.

**INTRODUCTION:**
In the times we are living in, passwords have become a serious and complicated topic. Nowadays it is far from just a phrase to be said out loud like in the middle ages when wanting to enter a fort or a building.

With the ever-growing collective consciousness and people mixing and mingling at so many different global platforms, it has become increasingly important to protect personal information. Yet, you cannot just grab a code or a word out of thin air and trust that it will suffice as a secure password to keep out the unwanted with ill intent and still grant you secure access when you have to use it.

Somehow, “Open Sesame” no longer cuts it in a world of strict cyber security, because the mere brute-force of an algorithm can make quick work of cracking the most creative password combinations.

With the ever-increased onslaught of phishing scams, cyber pirating and malware, the burden on the individual and businesses for the safekeeping of information have become particularly challenging. Trying to outsmart a criminal by composing a complex password that you are sure you would remember forever, frequently result in a forgotten password. Having to re-set it requires you to jump through a series of hoops to prove your identity in order to gain access to your own information. However, a robot manipulated from a remote location can access your information and steal your details to sell to the highest bidder, faster than you can execute a password change on your own system.

The irony is that you unintentionally, in the process of making your password as complex or clever as possible, end up opening it to vulnerabilities that enable the hackers to get their scaly digits on your priceless information.

Managing, memorising and organising passwords have become a burden that affects all of us. Just too many applications require passwords and you have to keep on relying on your memory. I am sure I am not the first (or the last) person who absentmindedly tried to heat up a plate of food by pressing one of my passwords from my overloaded memory into the keypad of the microwave oven. This is how bad the password-memory thing has become.

We live in an age where information overload has become a real problem and with all the different rules of different programmes and accounts relating to the creation of a password it is just impossible to keep dreaming up new safe “non-hackable” passwords with enough letters, digits and special characters that would satisfy the systems administrator.
Making all passwords the same, even if this was possible, is also not an option and exactly the reason why cyber risk has grown so much since the dawn of technology.

**So WHAT is the answer then?**
To get to the solution we must know exactly why passwords are so valuable, yet fallible in terms of security.

Where people use crude and easily guessable passwords people tend to be more prone to use the "remember this password" carrot available to them so conveniently, in the hope that they will not have to be annoyed and inconvenienced the next time that they access the application.

Since this practice has led to many security disasters, most employers do not prefer or even allow employees to use this option at all. Yet, you will still find the odd employee that does not have the time or energy to think up a secure password for each programme that he or she works on, who will click the remember password button with the pure intention to change the password as soon as the crisis is over. Especially in the Financial Industry, there is a multitude of platforms where multiple employees have to work on simultaneously, each with different password requirements. Then that "remember for me" box becomes all too inviting. It is thus important to take into account the human factor. Humans are working under pressure and they are fallible. Therefor the security measurements must be helpful and not a trap or hindrance.

Writing down a password is another huge risk. The challenge is that one may think you have creatively hidden it from praying eyes by incorporating it in the graffiti on your office wall, but believe me, when someone is set to find your pin, they will find it, even if they have to manually sort through an haystack, given the incentive is worth their while.

**Password Managers:**
So, the whole problem created by the above-mentioned risks has led to the development of risk mitigating strategies in the form of password protection management programmes for example LastPass (created by Marvasol Inc), which operates on browsing platforms such as Fire Fox, Google Chrome, Internet Explorer 11 and Safari to name but a few.

Here you get a password management service on what is known as a "freemium" licenced platform that means that you can access some of the services for free, but proper and more comprehensive password management services are available on a subscription basis at a fee.

These systems work on the basis that a user's content is protected by implementing a master password and it can then be synchronised with all devices the user frequents.
The information is kept in an encrypted form, which makes online attacks being successful, less likely.

Password management programmes also have the ability to flag cyber breaches and alert the user to change a password on a compromised platform before damage can be done to the user's data.

Password managers might not be the solution for everyone, yet, it has the potential to limit data breaches on billions of leaked accounts and that alone is a good enough reason to investigate the benefits and features of this tool.

Sites such as "Have I been Pwned" (HIBP) have been helpful in letting users input their e-mail addresses to see whether their e-mail service provider has been compromised in data breach incidents such as the recent Yahoo mail leak.

This has led to more password protection managers entering the market and a great demand has developed with especially the YouTube platform also recently undergoing an attack by hackers who breached the accounts of content providers and then held the data for ransom.

Pirating has taken on a completely new meaning in the digital era.

LastPass is not the only option in the user's quest for autonomy over personal information. Some of these Password Managers have been around since the 1990's and include among others:
Dashlane.com
KeePass XC
Enpass
Roboform
Bitwarden
Sticky password – created by the Developer of AVG virus protection.

Of course, there are many more and it is important to do proper research into the advantages and disadvantages of each Manager before entrusting them with your precious data.

A major possible downside to using a password management application is that the risk still exists of the Manager being hacked, hence the vital importance of proper option research. The popularity of some Password Managers automatically attracts the more opportunistic hackers, knowing that there is a great volume of information in one spot, increasing the odds of success with less effort.

Hackers are patient and they know that bombarding a system with a multitude of attacks will pay off at some stage, so it is imperative to limit the accessibility of data through employment of extra protective measures.

Multi-Factor Authentication, OTP's, Fingerprint scanning and password elimination:
Other innovations in the field of password protection are things like the development of fingerprint scanning technology, Multi-Factor Authentication and One-Time Passwords (OTP's). However all these endeavours to enhance cyber security does not safeguard against "phishable" methods.

There is a movement that advocates for the entire elimination of passwords, but the truth is that this will probably never be entirely viable. As long as data needs to be protected, a need for some sort of password / "gate keeping system" will continue to exist.

**Best practices:**
For all the reasons mentioned above, the focus should move from the love-hate relationship with passwords and encrypted data accessing measures, to the implementation of best practices to secure and protect passwords.
Some of the best practices can be summarised as follows:

- Adopt long passphrases instead of a word or a combination of words and symbols.
- Avoidance of periodic changes – the more something is changed, the easier it is for it to be compromised.
- Two-factor Authentication and advanced authentication methods.
- Creating a password blacklist.
- Encryption of passwords.
- Using only secure connections.
- Ensuring continuous backup of information.
- Additional protection of privileged users' accounts. Many systems only grant certain access to privileged and approved individuals to prevent data breaches by for example disgruntled employees. This is the same reason why the login details of a staff member who has left employment, must be revoked immediately to prevent misuse.
- Ongoing employee training to brief them on important system changes and strategies.
- Avoid storing passwords.

- Refrain from using dictionary words.
- Secure your cellular phone as this can also be stolen and used to access data and accounts using the Two-Factor Authentication method if not secured.

**Complexity can be the enemy of a strong password:**
According to NIST (National Institute for Standards and Technology), a complex password is neither a necessity for, nor a guarantee of a strong password.
Password testing tools like HashCat are very useful to easily do quality checks on passwords. Then there is Microsoft's "Risky Login" flag to identify users who log in to their Azure Active Directory with leaked credentials.

Password hints have also become redundant; because people can often not recall the exact answers to the "hints" they created years ago, not to mention the availability of information on social media platforms in today's society.

Your first pet's name might be common knowledge to all your friends and many more people purely because of the "Information sharing culture" we are finding ourselves in these days.

**Change is not always good:**
Although the instinct would be to regularly change passwords to avoid someone accessing it, NIST actually argues to the contrary. The more a password is changed, the more pressure it creates on the user to think up a new, original password that is still easy enough to remember, yet complex enough not to be guessed or brute-force-hacked. This is counter-productive and a major influence on why people create weak passwords or re-use passwords for multiple accounts.

**CONCLUSION:**
Password management services are more applicable to the general public, since businesses and Government Departments should have extensive risk management strategies in place which involve more stringent regulations and involvement of their IT departments. As demonstrated in this article through the explanation of other available protective measures it is also clear that Password Managers are not the be-all and end-all in this data protection battle. All of the measures should be applied and integrated as a holistic defence to the ever-increasing threat of data breaches.

Unfortunately, a vast portion of South African businesses are still ill prepared for this imminent hazard and sometimes it even takes as long as 48 hours before a company becomes aware that their security has been breached. 78% of South Africans acknowledge that they need to actively protect their information, yet the overwhelming perception still remains that security is an inconvenience. Prevention is however key to reduce the risk of financial losses or, worst-case scenario, possible ruin and that should override perceived inconvenience.

Knowledge is power and therefore it remains important to be aware of any dangers as well as benefits of a resource.

**Statistics and quotes**:
- "The more often you ask someone to change their password, the weaker the passwords they typically choose." – Dr Alan Woodward, University of Surrey
- In 2016 8.8million South Africans have already been victims of cyber-crime.
- Based on the Kinkayo Cyber Exposure Index's 2017 data, South Africa is tied with France, only topped by Finland in terms of the average exposure by country.
- "Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember and easy for computers to guess" Randall Munroe Creator of the web comic XKCD

**References:**
Camargue Underwriting Managers – Cyber risks
Smallbiztrends.com
National Institute for Standards and Technology (NIST)
Techspective.net – Marcell Gogan 23 May 2018
FA News magazine articles:

- October 2018 – The hidden costs in data breaches – Mojaphela Makau: Executive: Strategic Execution Enterprise Architecture & IT Tracker South Africa
- August 2018 – Could SME's be easy targets? – Christine Rodrigues: Partner at Hogan Lovells (South Africa) Inc.
- August 2018 – It will never happen to me – Heino Gevers: Customer Success Director at Mimecast

**Video resources:**
Who invented computer passwords (and the guy that made them suck) – Today I found out: YouTube
Password Managers Round-up – Second opinion #54 podcast by The Nexus: YouTube
The future of security keys: using your phone in the fight against phishing - Cloud next 119 – Google platform: YouTube
Top 5 best free Password Managers – Tech Gumbo: YouTube
Why passwords are actually important – Aaron Foster – TedX Colorado Springs: YouTube

# POLICY DEVELOPMENT WORKSHOP

### Overview By DoT OD Team

In March 2019, SAIMAS hosted a Practical MS /OD Policy Development workshop. The aim of the workshop was to provide SAIMAS members with information on how to develop a policy in their own organisations. The workshop was well attended by SAIMAS members. The workshop was facilitated by Mr Dirk Ehlers.

Policy is about change transformation in an organisation. Firstly, we need to establish that Policies are about people, the impact and changes that occur. Policy should be about how you do things. A good environmental policy is governed by good economic measures. Thus, there must be proper buy-in, communication and consultation from relevant stakeholders.

Mr Dirk Ehlers requested the attendees to list the day to day policies used by Organisational Development practitioners/ Work Study officers. The policies identified are listed below:

- Quality Management
- Job Evaluation
- Job Descriptions
- Microstructure development
- Change Management
- Business Process Management
- Structure
- Service Delivery
- Organisation Development

The attendees engaged in a session to discuss why policies fail and some of the reasons that were mentioned are:

- Decision makers don't understand the policy;
- Policies are not implemented and approved;

- Not user friendly;
- Not updated regularly; and
- Policies are not consulted effectively.

A policy is there for guidance. They also seem to fail because of political interference, interference from external sources, budget issues and no accountability. He emphasised that Departments must have a policy on policies of which a template was sent to workshop participants, to develop their own policy.
The following reasons were provided on why policies fail:

**Reasons policies fails**

- Lack of crisis perception by policy-makers
- Ideological, rational and emotional resistance
- Lack of support
- Legal obstacles
- Communication and lack of implementation strategy
- Lack of resources
- Honesty and integrity

In order to mitigate the possibility of policy failure change strategies were discussed and are listed below:

**Change resistance strategies**

- Tactical application of sudden or gradual change;
- Use technology that minimises resistance;
- De-legitimise the old system by legitimising the new system;
- Use innovation adoption rather than termination and or succession plans;
- Create a win-win scenario;
- Use windows of opportunities to initiate the change;
- Apply sound Management practices. e.g. Risk and change management;
- Transparency, honesty and participation and change processes;
- Structure and process change are easier to manage than behaviour and attitudes;
- Peripheral values change more easily than core values.

A Policy must be SMART- Simple, Measurable, Attainable, and Realistic and have a Target.

**Reasons for Policy changes**

- Changing external environment;
- Changing stakeholder requirements;
- Changes in demands of Government;
- Changes in resource base;
- Changes in Institutions;
- Change of political Leadership; and
- Changes in Service Delivery Strategies.

A Procedure document is written to support a policy directive and is designed to describe who, what, where, when and why by means of establishing corporate accountability in support of the implementation of a policy.

Policies are identified according to levels; level 0 is Government policy; level 1 is Departmental policy; level 2 is Branch policy and level 3 is Divisional policy.

The Governmental policy authority is the Government and must be applicable to Government Departments and supported by Executing Authorities. The Departmental policy authority is the Head of Department and must be applicable to all Branches and Divisional Heads and supported by Divisional Heads. The Branch policy authority is the Branch policy owners and must be applicable to Divisional Heads and supported by Unit managers. The Divisional policy authority is the Divisional Heads and must be applicable to Unit managers and supported by Business Process Owners.

The policy hierarchy differentiates all kinds of policies ranging from laws (acts), regulations, policies, standards and practices, procedures and guidelines. Practices, standards & Guidelines can be changed e.g. if Job Evaluation practices change, then the technical policy and technique can be supported on high level. Laws guides us in terms of what to do or how to act and Regulations refers to how things are done.

The Policy directive purpose is to communicate information about policies, procedures and processes relating to matters overseen by the Department responsible for Administration and its divisions. Each division is responsible for administering its own policy directives.

### Mandate VS Policy

A Mandate is derived from an act or a law. We also need to analyse the statutory mandate to determine group policies. Mandate vs policy have got four pillars which are Authority, Purpose, Structure and Performance. Authority has to do with someone taking responsibility for their actions. Purpose helps with strategic direction of an organisation which makes it easy for policy decision makers. Performance is the outputs and outcomes. Project owners present the policy to the unions.

### Roles of the policy development team

- Create a climate of participation;
- Organise resources;
- Create ownership and accountability;
- Formulate the basic concepts;
- Scenario setting;
- Stakeholder acceptance;
- Communications and feedback; and
- Project management.

Directives must be able to share information and communicated loud and clear.

### Directive Guidelines

With regards to the Guidelines, one needs to clearly state or indicate what needs to be done and give as much detail as necessary for the tasks, projects, or other assignments that needs to be accomplished. If a problem needs to be resolved, clearly indicate what the problem is and if desired, how would you like it to be resolved. Reasons must be given for directives, with specifications stating how the reader should proceed in order to accomplish the task. Clear deadlines for the completion of the task or project should be given. Arrange for follow up or evaluation if needed. Mention the benefits of the directive to the people involved. If appropriate, offer to give assistance if needed or offer any answers to any questions or problems that may arise. Lastly thank the reader and close the session by expressing your confidence that he or she can complete the task at hand.

Visit the SAIMAS website to download the templates referred to in the overview

# TEAM BUILDING

**By Boitumelo Kamba**

### Introduction

The reason why most organisations embark on team building is to encourage trust in the workplace. Working relationships must be strengthened and morale boosted. Collaboration between management and employees must be strengthened as it can seem as if it is non-existent.

In my current workplace, there are a lot of gaps in terms of who does what. Even though each team member has their own job description, roles are not clearly defined. This situation can be avoided if the unit allows themselves to function as a team instead of maintaining an ‘INDIVIDUALITY SYDROME” with ONLY I CAN DO THIS ‘. This scenario does not allow for skills being transferred and often team members have differences with their supervisors and peers, resulting in conflict situations which disrupts a healthy working environment.

To deal with this tendency, Team Building should be introduced which will help employees to open up on the issues bothering them. It is vital that employees share their dissatisfactions. Keeping issues to one self is not the answer. Many employees are unhappy with how they are treated at work, which is triggered by them feeling unappreciated for the efforts they put in, or feeling overlooked and not thanked for their contribution. If one works in an environment where there is no trust, honesty, openness and transparency, there will not be harmony in the workplace. Sharing concerns and voicing opinions must be the start of better and greater harmony.

We all forget that an organisation does not consist of squares on a piece of paper but of people. Management should invest in their employees because without them not much will be achieved. Employees need to be motivated which will help to them excel in their roles and responsibility. When employees are happy, they are more productive. Turnover rates are normally reduced when employees are happy with their working conditions and surroundings.

### What is Team Building

Team building is the process of a group of individuals contributing towards a solid and unified team. A team is a group of people structured to work together interdependently, supportively and willingly to **meet** the needs of their clientele by accomplishing their purpose and goals.  Partnerships and cooperation are key to how businesses and organisations operate, with individuals sharing their skills and awareness and understanding to complete mutual beneficial tasks.  At its best, team building can have far-reaching positive results. However, the process of encouraging team building can be costly and ineffective when business leaders fail to perform it properly especially if they are short sighted. It is equally important that team building can facilitate other Organisational Development interventions such as employee involvement, work design, restructuring and strategic change management.

**Better Communication**

Enhanced and enriched communication is a positive result of a successful team-building program. Workers who learn to efficiently and effectively complete shared tasks in a controlled setting are better able to converse and interconnect with facts in relation to accuracy on the job. This extends not only to verbal communication but also to recognising one another's needs and limitations. Strong communicators have a chance to move into team leadership positions where they can help others fuse, blend and share information. Team building can also cause employees to be more patient with one another, decreasing the risk of misunderstandings.

**Higher Efficiency**

The net result of team building that most businesses hope for is enhanced efficiency. When team members are able to remain focused on group goals and they rely on one another's strengths to compensate for weaknesses or areas that need improvement, they can complete tasks quickly and professionally. Team building can also increase morale be removing personal barriers that existed before the team building exercises or education and this also leads to greater productivity from individual members and the team as a whole.

**The results of team building**

Team building's effectiveness has produced inconsistent results and the reason is that employee's openness and decision making is often taken for granted. Team building is a process that takes place over time it does not happen instantly.  Team building is directed towards improving group effectiveness and the ways in which members of teams work together.  Teams may be permanent or temporary or traditional or virtual, but either one them have common organisational aims or work activities.

**Conclusion**

| TEAM ADVANTAGES | TEAM DISADVANTAGES |
|---|---|
| • Team members have the opportunity to learn from each other. | • Some individuals are not compatible with team work. |
| • Potential exists for a greater work force flexibility with cross-training. | • Workers must be selected to fit the team as well as have the requisite job skills. |
| • Opportunity is provided for synergistic combinations of ideas and abilities. | • Some members may experience being less motivated doing the job when part of a team. |
| • New approaches to tasks may be discovered. | • The organisation may resist to change. |

| | |
|---|---|
| • Team membership can provide social facilitation and support for difficult tasks and situations. | • Conflict may develop between team members or other teams. |
| • Communication and information exchange may be facilitated and increased. | • Teams may be time-consuming due to the need for coordination and consensus. |
| • Teams can foster greater cooperation among team members. | • Teams can stymie creativity and inhibit good decision-making if "group think" becomes prevalent. |
| • Interdependent work flow can be enhanced. | • Evaluation and rewards may be perceived as less powerful. |
| • Potential exists for greater acceptance and understanding of team-made decisions. | • "Free-riding" within the team may occur. |
| • Greater autonomy, variety, identity, significance and feedback for workers can occur. | • Less flexibility may be experienced in personnel replacement or transfer. |
| • Team commitment may stimulate performance and attendance. | |

**Reference List**

**Brown D.R. & D. Harvey (2006) Experiential approach to development: (7th ed.)**

**Cummings, T.G. & Worley, C.G (2015) Organisation development and change (10th ed.).**

**Martins, N. & Geldenhuys, D. (2016) Fundamentals of organisational development (Eds).**