TIME FOR A RETHINK – SECURITY HAS FAILED TO EVOLVE BASED ON USER ROLES AND RESPONSIBILITIES

Author: Rizwan Mahmood

Published: August 2017

1 SYNOPSIS

User behaviour accounts for over 50% of information leaks, based on various studies, and yet traditional security systems have failed to solve the problem. The fundamental reason for these failures is the treatment of users as “kids”. We believe it is time to trust end-users and give them the freedom they require to do their job whilst making them responsible for how they use sensitive information.

This paper reviews information security in light of McGregor’s[i] Theory X and Theory Y human motivation and management principles. Use of the Theory X approach, the aim of which is to micromanage end-user access to data, explains the limited success of traditional security solutions such as UEBA, SIEM and DLPs. This is contrasted with the Theory Y approach, as realised in People-Centric Security (PCS), which allows end-users more freedom.

Finally, e-Safe Compliance is introduced to demonstrate how the principles of PCS can be implemented in practice to provide a fundamentally different implementation approach to existing, traditional security solutions.

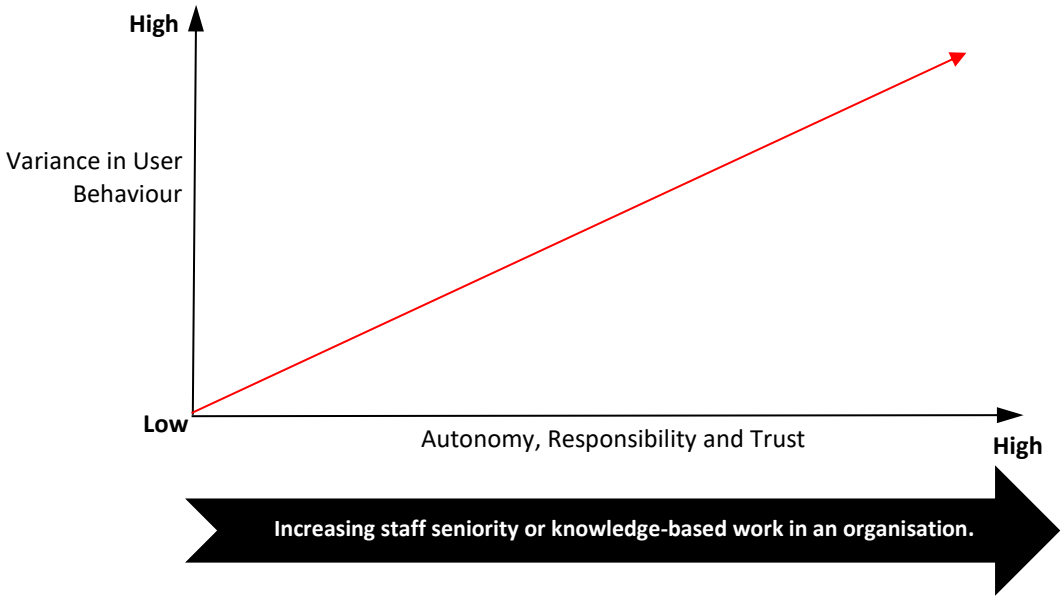
2 TRADITIONAL SECURITY HAS FAILED TO EVOLVE BASED ON USER ROLES AND RESPONSIBILITIES IN AN ORGANIZATION

Theory X and Theory Y are theories of human motivation and management created and developed by Douglas McGregor in 1960. Theory X assumes that employees are naturally demotivated, dislike working and avoid responsibility. They need to be supervised every step of the way with controls in place. They have to be threatened and forced to deliver what is needed. Theory Y is the direct opposite of Theory X. Theory Y assumes that employees are happy to work, are self-motivated and creative and enjoy working with greater responsibility. In comparison to "Theory X", "Theory Y" gives the work force more of a feeling of democracy and freedom.

Application of the Theory X and Theory Y style of management greatly depends on the type of users. Although Theory X is widely considered as an inferior management technique, it is highly effective in a production environment which requires repetitive, **PREDICTABLE** tasks to be performed with little to no decision-making, normally associated with junior staff members. Whereas Theory Y style of management is more suited to knowledge workers, and people in professional services and management positions, have greater responsibilities, face decision-making and deal with the varying nature of challenges. The

increased autonomy in making decisions results in Theory Y users having a much higher level of behaviour variance and **UNPREDICTABILITY** than Theory X users as shown in the Figure 1.

FIGURE 1: VARIANCE IN USER BEHAVIOUR BASED ON USER ROLES



To date, the current security technologies have been based on the Theory X view of the entire organisation. They are based on the idea that the sole responsibility of ensuring security rests with central security. As such, central security should be given the tools to control "THEM" - the end-users who are considered to have to be controlled, forced and threatened to stay on course.

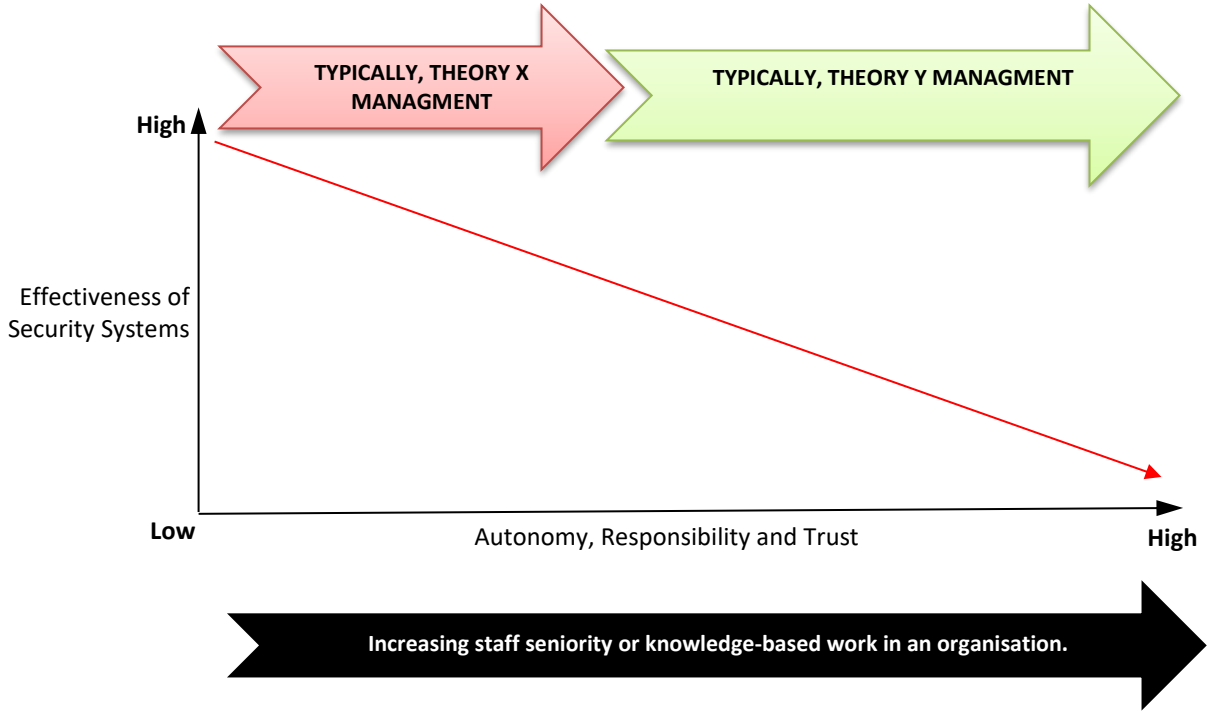
This course of action has found success in areas of organisation which do repetitive and more of the assembly line style of work, i.e., by junior roles in an organisation. Applying strict controls to these users, using technologies like UEBA, EM, DLPs, SIEM, blockers and filters, produces good results as any **variance in behaviour** can easily be mapped and these users can be forced to follow a certain policy, like no bulk copying of sensitive files to a USB drive.

Unfortunately, application of the Theory X style of security management to management staff, information owners, and knowledge workers (in research firms, law firms, professional services, etc.) has had little success. The primary reason for this is the unpredictability of user behaviours in these roles due to the higher degree of autonomy and trust they enjoy while performing their jobs. Users at these levels are generally managed using the Theory Y management style.

However, when it comes to security, instead of managing them as Theory Y users, they are treated like Theory X users. They are forced by the IT security teams to follow certain controls without any mutual trust and responsibility. Considering the higher level of influence which these users have, this results in a power struggle, with IT security mostly ending up on the losing side. For example, when restricting the

use of Dropbox or a USB drive by a CFO when he genuinely wants to take his work home due to a deadline, the CFO always WINS, but this allowance opens up a security threat and auditing nightmare as IT security will not have any idea whether any future actions will be for legitimate reasons. Figure 2 illustrates the diminishing effectiveness of security solutions in this scenario.

FIGURE 2: DIMINISHING EFFECTIVENESS OF SECURITY SOLUTIONS



The power struggle between IT security and information owners (senior members) in organisations has resulted in serious security issues for the entire organisation as follows:

1. **Identification and classification of key assets** → famous frameworks and standards like NIST and ISO27001 rely on this fundamental process for success and so does every security system. Unfortunately, the identification lies solely with the information owners. Forcing the information out of information owners who do not see their responsibility in providing it or have any interaction with the result of the classification on an on-going basis is one of the hardest challenges faced by IT security. Failure of this process means **NO SECURITY**.
2. **Getting Top Management Commitment** → top management commitment to the security programme is the fundamental requirement of any project. However, it is easier said than done. IT security struggles to win them over by showing them graphs and matrices containing information which they do not really understand as they are not part of the actual process. In the end, they are required to take a leap of faith, which, depending on the company's financial position, may get lowered in priority.
3. **Privacy vs surveillance, who wins**? → one of the key tools used to monitor user behaviour is IT surveillance or monitoring of some form. This raises privacy concerns in an organisation. Although the privacy concerns are there for junior staff, they gain much more prominence as these tools

are applied to monitoring the senior management. Monitoring these users is of utmost importance as they are responsible for handling really sensitive information but convincing them that someone in IT security (typically their junior) should be monitoring their every move is a whole different matter. IT Security mostly ends up on the losing side. In many cases, requests to not monitor them are for genuine reasons, for example, when HR is working on bonuses or C-level staff is working on retrenchment plans. Unfortunately, it also means that the most sensitive information never gets protected.

4. **"Cry wolf Scenarios" - too many alerts results in complacency** → when it comes to monitoring information owners and management, traditional technologies like SIEM, employee monitoring, UBEA, DLPs have all been responsible for producing too many false hits. In most cases, actual leaks are detected by one of the systems but, due to the sheer number of alerts, IT security has no idea whether the alerts are genuine and eventually, they get overlooked. These unfortunate cases have resulted in the change of purpose for the security systems from **prevention** to **after-the-damage** forensic systems, only to be used once IT security comes to know of a particular leak from the newspapers.
5. **Analytics and Machine learning have limitations** → they are being touted as the next big thing, which will help in solving the user behaviour issues without actually interacting with the end-users. The way they work is based on defining a regular user pattern and alerting if the user does something drastically different from his normal working behaviour, like copying 100s of files. Unfortunately, these techniques fail if the leaks are a result of normal or usual behaviour, for example, a privileged user copying a single file, i.e., due to **low risk events**. Further, if the initial behaviour used to define the pattern is already bad or highly unpredictable in the case of information owners, the hits are highly irregular, resulting in a high degree of false hits and not much security.

3 THE ALTERNATIVE → PEOPLE-CENTRIC SECURITY. A SOLUTION FOR SECURING THEORY Y USERS.

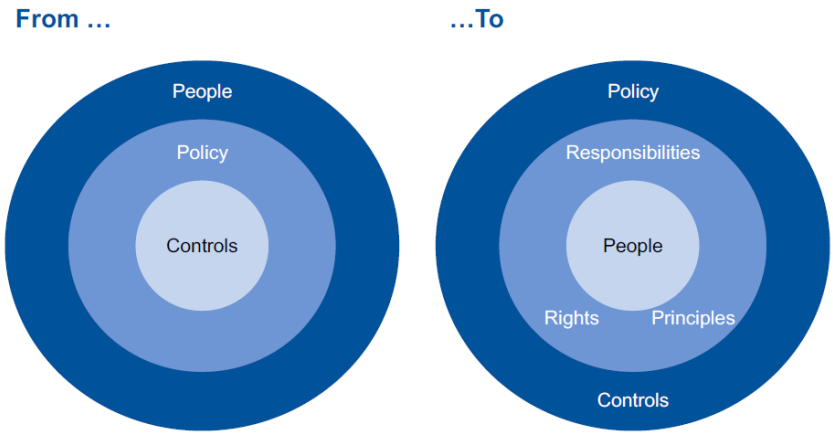
The concept of People-Centric Security was first introduced by Tom Scholtz[ii] of Gartner in 2012. Tom proposes a more "*trust-based security strategy, founded on a set of key principles, and based on mutual rights and responsibilities of individuals, is a viable alternative to the status quo. Such a PCS approach places more direct responsibility and trust on individual users.*"

It is based on the assumption that most individuals intuitively want to behave in an appropriate manner and want to work for the benefit of the business rather than being inherently evil. PCS moves from a control-centric security approach to a people-centric security approach as shown in Figure 3 and one that is based on TRUST BUT VERIFY with user education and understanding at its core.

The concept of PCS is very much in line with the Theory Y management style and that is why it is a much more natural alternative for the users who are already being managed using this style of management, e.g., knowledge workers, information owners, professional services people and management staff.

The PCS approach gives the Theory Y managed users the rights they desire to get the job done but that does not mean they have a free hand without being monitored. In fact, the level of monitoring increases under PCS but with a major difference. Instead of being control- or block-driven, it is mostly detective and passive monitoring in nature. This allows for greater flexibility and freedom for users to carry on their job in line with the TRUST philosophy.

FIGURE 3: PEOPLE-CENTRIC SECURITY



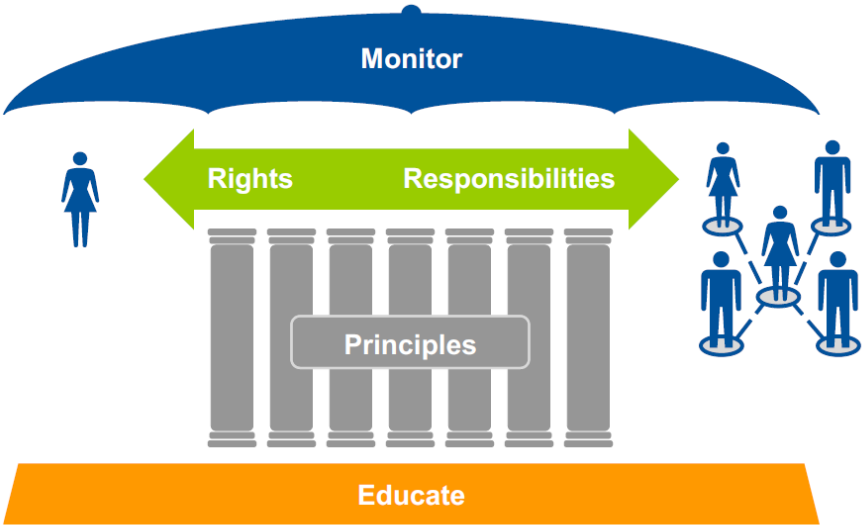
Source: Gartner (September 2012)

However, this higher degree of autonomy comes with a price as they are now held responsible and accountable for the security of the information they handle, which is in line with the VERIFY philosophy. In the event the trust is broken, stricter controls could be brought back in. However, the punitive actions are not organisation-wide like in the current, traditional security systems but are user-based.

The increased rights and responsibilities of users and the changes in monitoring philosophies under PCS are governed by seven principals, as defined by Tom Scholtz [iii], which are:

1. Accountability
2. Responsibility
3. Autonomy
4. Immediacy
5. Community
6. Proportionality
7. Transparency

Figure 4 showcases the 7 PCS Principals[iv] as pillars on which PCS framework is based.



Source: Gartner (August 2014)

4 IMPLEMENTING PCS USING E-SAFE COMPLIANCE

The following section showcases a practical implementation of PCS principals using e-Safe Compliance.

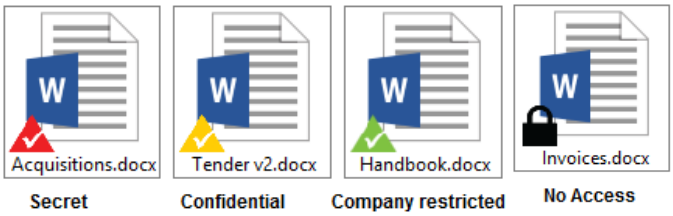
4.1 ACCOUNTABILITY → ENSURES CLASSIFICATION AND PROTECTION OF SENSITIVE INFORMATION BY OWNERS

e-Safe Compliance, through user empowerment, makes the information owners accountable for the protection of information they are responsible for by creating roles for them in the system. Using these roles, they can now classify the information themselves and, more importantly, define how it should be used. Information owners receive reports on the usage of their information and can make the call if it is not used appropriately.

The classified information is sent to the central IT security, who then implements the necessary controls as suggested by the information owners. This ensures that information owners do not have a high learning curve in terms of classifying and securing their information. The accountability of the IT security team now moves from being the auditor of information to auditor and facilitator of the actual, decentralised security process

The following are some of the ways information can be classified by the information owners using the specialised, decentralised data classification tools:

1. **Classification by virtue of sensitive words, file names, regular expressions** → information owners can create their own rules based on the information they are responsible for, along with how it should be used using information usage restrictions.
2. **Classifying information stores** → most of the information created by information owners is either stored in document management systems like SharePoint, in databases and in shared folders. Information owners can mark the content of these information stores with the relevant importance using e-Safe. Once marked, e-Safe scans these stores on a regular basis to auto-classify any new information being created in these stores.
3. **Auto-generation of sensitive words** → asking the users to define sensitive words is a tough ask and it could be time-consuming. As such, e-Safe offers a specialised tool that automatically extracts unique words from a similar set of documents. These words can then be fed into rules and be monitored across the board.
4. **Document rights management Module** → documents and files are still the most common form of sensitive information in an organisation. Users can simply right-click on particular documents to define their classification levels. The classified documents are also secured using persistent encryption which follows the document. Further, they can also define access rights for those



particular documents. The classified documents are represented by a visible, triangular icon. The visible indicator serves as a visual warning to the users that these documents are sensitive and are being monitored.

4.2 RESPONSIBILITY → SHARED RESPONSIBILITY LEADS TO HIGHER SECURITY

e-Safe Compliance does not adopt a blocking approach to security but instead adopts a more flexible monitoring approach based on **responsible use of information**. Under this approach, the usage of information is based on the sensitivity of the information as defined by the information owners. However, the users are allowed to make a judgement call and are held responsible for their actions. The approach is implemented using the traditional technologies of **user behaviour analytics** and **employee monitoring tools**. However, there are fundamental differences in how these technologies are implemented in light of PCS, which are as follows:

1. **Monitoring based on classification** → users are monitored based on the information sensitivity and risks defined by their information owners. This ensures monitoring is more targeted and proportionate to the risks involved with specific information. Further, the classification helps to limit exposure of private user information, hence helping to **balance off privacy concerns**.
2. **Nothing is done in a hidden manner** → users are informed that the usage of company information is being monitored.
3. **Information owners are made responsible for their information** → **t**hey receive reports on the usage of their information by users and are responsible for highlighting any misuse. This ensures leaks or mistakes due to normal working behaviour can be picked up.
4. **Selective reporting on Top Management removes their privacy concerns** → the e-Safe Compliance reporting workflow allows the flexibility that reports regarding senior members of the company can only be seen by the designated authorised authority in the company, for example, by the Head of Internal Audit or even the CEO. This flexibility ensures that senior management have the assurance that highly-sensitive information is monitored and remains within the circle of a select few.
5. **Privacy and education are ensured** → each user gets an individual report. The report is meant to educate the user by highlighting potentially risky actions and that he is also held **responsible for his actions**. Further, the report ensures the users are made aware of the information that has been captured by the company, hence fulfilling the requirement under the privacy laws.
6. **IT Security is the facilitator and educator rather than the enforcer** → the primary responsibility of IT Security is to facilitate and audit the running of the distributed security process used by the relevant parties. Further an important part of their workload now moves to that of an educator, who answers queries raised by users on particular risks identified in their reports. This interaction helps to quickly raise the security awareness level among the general population of users.
7. **Reduced load for IT security means better security** → the number of actionable reports is reduced for IT Security. IT security still receives generic trend reports and standards compliance reports for PCI DSS, Privacy Act, GDPR, etc., but the reduction in load means they can now focus on these reports.

8. **Operationalisation of Security makes for easy cost justification** → everyone in the company gets engaged with security, which means security is no longer the black hole which no one understands but instead it becomes a part of their daily lives. e-Safe Compliance sells itself to the top management.

4.3 AUTONOMY → MORE FREEDOM THROUGH TRUST AND SELF-GOVERNANCE

e-Safe Compliance fosters a culture of Trust and Self-Governance among the staff. Users make the call on the usage of the information based on their responsibilities. For example, a finance executive working on a last-minute, next-quarter financial could decide to take it home via USB drive or Dropbox as long as he gets authority to do so from the information owner, the CFO in this case. The finance executive knows that if he does not do that, the CFO will receive the report of his activity and might start an enquiry.

e-Safe Compliance further assists in this autonomy and flexibility by providing targeted encryption of sensitive files. Once encrypted, they can be transferred using any means, e.g., free cloud services and USB drive. The encrypted files can be accessed on any device which has the e-Safe's encryption-only agent installed. This ensures flexibility along with complete security and accountability of the sensitive information.

4.4 IMMEDIACY → USER EMPOWERMENT REDUCES DETECTION TIME AND IMPROVES USER EDUCATION

The primary focus of empowering the users by using e-Safe Compliance is to reduce the "Detection Time" of a transgression. By decentralising the reporting of transgressions to people who understand the sensitive information, it is ensured they are picked up quickly and remedial steps can be taken immediately.

As the reporting is user-based, companies can decide whether to educate the users or, if the action is deliberate, to take more aggressive, punitive actions.

Further, as all users are aware of and can view their own actions/transgressions, in the event they still continue down the wrong path, companies have all the evidence and justification to take action against the involved individuals.

4.5 COMMUNITY → FOSTERS A CULTURAL CHANGE TOWARDS SECURITY

One of the biggest challenges faced by security teams is to develop a culture of security in the organisation. Through decentralisation of security roles and responsibilities, e-Safe Compliance ensures all users starting from top management to junior executives are involved in the decision-making and are responsible for how the information should be used and processed. The added responsibility upon the management ensures that they lead by example for their teams. This facilitates an overall cultural change in the organisation towards security.

Further, e-Safe Compliance also provides the option to produce overall risk scores based on department. Security teams can decide to publish the departmental risk scores, resulting in gamification of security compliance by pitching different departments against each other. This healthy competition instils a sense of teamwork to improve security among the users, so as to ensure their department is not at the bottom of the list.

4.6 PROPORTIONALITY → FOCUSED MONITORING VIA DATACENTRIC SECURITY

The freer handling of the information due to greater autonomy allowed under PCS is verified using e-Safe Compliance's advanced monitoring features which are proportionate to risk involved. e-Safe Compliance works on the principals of total visibility of sensitive information and Data-Centric security. Unlike many existing security technologies which either block or allow an entire medium, e-Safe Compliance focuses on protecting the data while giving total visibility to the responsible users. This ensures users are not burdened by unnecessary security but still have the flexibility to do get their job done. Some of the specific features include:

1. **File-centric security → f**iles and documents are protected using transparent and persistent encryption, meaning the encryption remains with the files irrespective of the medium and is offline ready. Users can then share the files using any means they prefer, which includes free cloud services and free email services, or work from home as long as they have the e-Safe agent installed. Further, access control can be applied to these files, ensuring only authorised users have access to the files.
2. **User -based settings →** user profiles and groups ensure different settings for different groups of users based on responsibility and accountability.
3. **Overriding principal →** Privileged users have the option to override print and copy restrictions on a particular sensitive file as long as they give a reason. The reasons are sent to the information owners for verification.
4. **Monitoring information in stores →** e-Safe Compliance scans the information stores and databases (using SQL) and classifies sensitive information stored within them. This information is then monitored for its usage as defined by the information owners.
5. **Monitoring at the end-point ensures total visibility →** e-Safe Compliance achieves total visibility on the usage of information by monitoring information at the point of use (end-point). This ensures it is not affected by encrypted transfer of the information via proxies, encrypted chats, free email services, etc. The report contains full detail of the transgression including the context in which it occurred. For example, if GMAIL was used to transfer information, the complete body of the email along with complete recipient details are captured for evidence purposes.

4.7 TRANSPARENCY

e-Safe Compliance is built on the philosophy of TRUST BUT VERIFY. All monitoring is done in consultation with the specific departmental heads and information owner groups. The system deploys these settings based on specific user profiles which are configured as required by that user group.

e-Safe supports dual reporting in line with ISO27000, which ensures that all reporting is always looked at by more than one person. This not only ensures better security but also ensures transparency and fairness of any punitive action. Further, e-Safe also offers options to send individual users their risk report. As such, users are always aware of what is being monitored, which is in line with privacy laws. Further, this helps to educate the user regarding their risky behaviours.

5 RECOMMENDATIONS

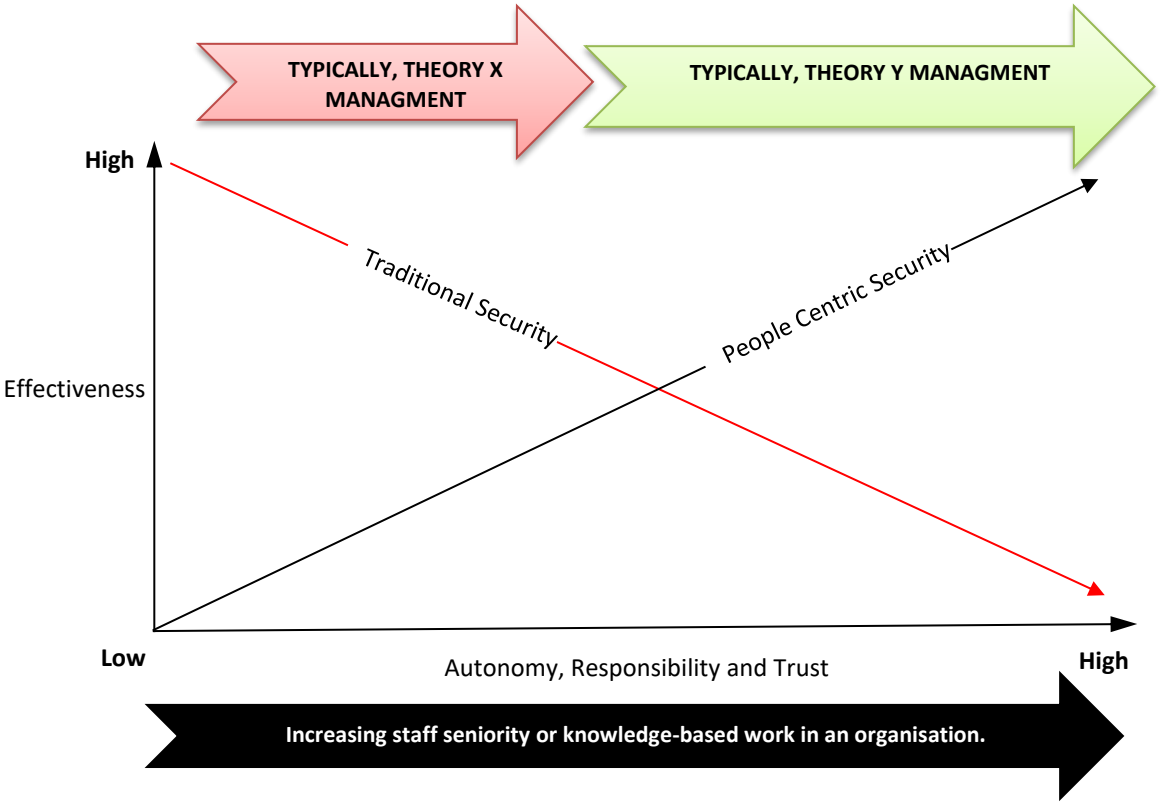
5.1 NEED FOR A HYBRID APPROACH (TRADITIONAL AND PCS)

As has been argued, PCS-based implementation models work best with users who are managed using Theory Y management principals. Applying PCS to junior staff or highly-regulated job roles which are currently being managed using Theory X management style will result in management overheads as they do not require the high levels of autonomy and responsibility, which form the bedrock of PCS. As such, it is better to manage them using the tried-and-tested, traditional security methods.

As most organisations will have both kinds of users, it can be argued that an ideal security implementation would consist of a **Hybrid** approach, incorporating a combination of both traditional and people-centric security. PCS in this hybrid approach would be implemented depending on the roles and responsibilities of the users within an organisation as shown in Figure 5 below.

e-Safe Compliance can be set up in this Hybrid configuration as it supports both traditional security and PCS-based implementations. Its various modules of UEBA, data classification, employee monitoring and information protection can be set in a highly-centralised monitoring and management structure with strict guidelines for certain groups of users within an organisation while following the PCS principals for the rest.

FIGURE 5: A HYBRID APPROACH



5.2 STAGE-BASED IMPLEMENTATION

PCS requires a dramatic rethink of the existing security implementation. It requires thorough planning as the correct people must be identified, who in turn should be trained on how to classify information and handle the increased set of responsibilities given to them. As such, a staged-based implementation approach is advised. The stages can be limited, based on high-risk departments or by scale of information that will be covered initially, i.e., coverage limited to certain data stores.

6 ABOUT THE AUTHOR

Rizwan Mahmood is the Director (Projects) for e-Safe Systems - a UK-based security company specialising in preventing security threats arising from human behaviour. Rizwan has 16 years of experience in the R&D of information security and artificial intelligence-based systems. He holds a Masters in Information Technology Management from Staffordshire University, UK and is a certified Project Management Professional (PMP®). Rizwan's areas of expertise include managing security threats arising from user behaviour, operationalising information security, image processing and resource optimisation algorithms. He has been involved in design and development of a wide variety of security systems (comprising both physical and digital) used by many organisations, including law enforcement and defence forces.

Rizwan has been involved with e-Safe Systems and its products from inception and set up and managed the global research and development facility for e-Safe Systems in Malaysia before moving to Australia. In his current role at e-Safe Systems (Australia), he is responsible for establishing the strategic direction for e-Safe System's security products in light of the new security challenges and market needs.

7 REFERENCES

[i] McGregor, D. (1960). The Human Side of Enterprise, New York, McGrawHill.

[ii] Tom Scholtz, GARTNER (2012). Maverick* Research: Kill Off Security Controls to Reduce Risk (https://www.gartner.com/doc/2156018/maverick-research-kill-security-controls)

[iii] Tom Scholtz, GARTNER (2014). People-Centric Security Principles Template

[iv] Tom Scholtz, GARTNER (2015). Toolkit: Sample PCS Principles, Rights and Responsibilities Templates