Intelligence-led design in security:

Technology-enabled security officers for the future

A G4S White Paper

January 2014

Preface

This G4S White Paper is intended to map out Secure Solutions' views on the future of 'intelligence-led design' in security systems and operations. By intelligent design, we mean the construction of systems that fuse security with a hand-in-glove understanding that intelligence is the key to an effective security operation. In particular, we offer the view that the future of intelligence-led design in security is personnel enhanced and enabled by an approach to technology which sees the effectiveness of both officer and systems as closely interlinked.

Our paper is not an exhaustive expression of our vision on this topic. Instead, it is intended to be a catalyst for debate, discussion and wider dialogue on technology-enabled security officers, as an emerging best practice standard in the security industry. Moreover, in this paper we seek to thematically explore the benefits that such an approach can offer to industries which rely upon an efficient and effective security regime for its protection.

Much in the same way that an officers' torch and log-book would be the old traditional tools for the job, we are scanning the horizon for what G4S Secure Solutions sees as the future. Namely, that security officers will increasingly find technology, backed up by appropriate systems and processes in incident capture, analysis and solution-design, as the new indispensable tools with which to deliver security. Consequently, we believe that customers will see this as indispensable too.

Essentially, there has been for some time a polarisation of views on the above, and this divergence of views can be described as the debate between the 'traditional' and the 'new model for security'. Almost all of the diverse security industry appreciates this, and this variance in opinion has been taking shape for a while now. However, a definitive way forward has not yet been found.

Our White Paper aims to help this definition take shape through the prism of what we call intelligence-led design and technology-enabled officers. Do share this paper with colleagues and industry contacts who may find it thought-provoking. Innovation is dependent on debate and discussion.

This paper seeks to prompt all three.

Table of contents

‘Total’ security – what is it, and how do we get there?

It has been argued by some that ‘security’ is a neglected and even ill-defined concept[1]. On reflection, we argue that this may not be an altogether unfair analysis. The concept of security, within the security industry and among its wider stakeholders, can sometimes be taken for granted. This therefore poses the question, what do we mean by security per se?

The traditional and standard observation of security as a concept would be that it is the prevention and mitigation of danger, risk, damage and/or loss to individuals or entities. When placed into practice as an industry, security is in its most basic form viewed as the provision of personnel, CCTV equipment, alarms and other services to encapsulate this common perception of security. Specifically, in the industry in which G4S Secure Solutions operates, this is most often expressed in security officers as a service complemented by other services, for example the provision of equipment and systems.

The archetypal image of the traditional security service is well-known: an officer guarding a site, venturing from a control room to investigate incidents, keeping his duty log updated, doing his rounds when agreed, and dealing with incidents appropriately when they occur.

Of course, this is all true, or at least was. The provision of security officers is a fundamental part of the offering but it is simplistic and does not capture the subtleties and complexities of this corner of the industry, nor does it fully encapsulate the direction in which it has been moving, and continues to move.

Increasingly in the past, it would also be fair to say that too often the ‘traditional’ model of security – via the kind of illustration we have provided – could be interpreted as typically a reactive service, ie., dealing with incidents when they arise.
We ask this question, is this ‘total’ security?

The reason for asking is that often it may be the case that by the time a security service has sprung into action – reactively - a breach of a secure zone, damage and/or loss may have already been sustained and that subsequent security activity is mitigation. This may be described as ‘partial’ security, as we have already outlined, and therefore a ‘reactive’ approach to security. We offer the view that it is necessary to examine this partial/reactive expectation, and to look into whether a ‘total’ or ‘proactive’, even ‘pre-emptive’, approach is the best way forward – for both the industry itself as well as for those reliant on its services.

Underpinning this examination is the fundamental question: is it enough to simply deal with incidents when they occur? If that is the express strategic intent of a recipient of security services, then of course, yes it must be. But if we are looking for solutions, and not just reactions, a more comprehensive understanding of security must be sought. In our view, and for the purposes of discussion, let us refer to this as a ‘total’ approach.

By total, we mean a before, during and after understanding of security and the risks/threats facing it. Returning to our earlier attempt to define security per se, we settled that it is the prevention and mitigation of dangers, losses, threats etc. In order to break this down, perhaps the following definitions are helpful: -

- Before = Prevention.
- During = Mitigation.
- After = Analysis and post-incident solution design.

This is what we would call a ‘total’ approach, the circularity and interdependency of the three is obvious. Of course, many practitioners of security will insist that this is what is done already, and has been done for years. This is no doubt true but in our view a key ingredient is either lacking, or missing altogether.

That ingredient is the seamless fusion of people, process and technology.

Understanding that there can never be such a thing as literal total security, when we look at our

[1] The concept of security, David A. Baldwin, Review of International Studies (1997)

definition of ‘total’ security as *before*, *during* and *after*, we believe the answer on how we get there is what we call the intelligence-led design of security.

Intelligent design in security solutions

At G4S we believe in the time-honoured adage that knowledge is power. Nowhere is this more correct than in our view of intelligent design in security solutions.

In our definition of total security, we have sought to design a three-pronged illustration of security in a timeline format. To do so, as in the previous section, we defined the timeline as before, during and after incidents, with the security translations of these three stages as prevention, mitigation and post-incident analytical solution design, respectively.

We offer the argument that for a proactive total approach the most important stage in our three-pronged illustration is ultimately the latter, after/analysis and solution design. This is because at this stage, an appropriate and comprehensive approach can help to design preventative measures prior to incidents, and shape the most effective mitigation tactics and strategies should they occur. This, we argue, is the lifeblood of intelligence-led design.

If we maintain that prevention is better than cure (as we surely do), a total approach will require effective, efficient and intelligent identification, reporting, tracking, management and analytical processes. In short, it requires a comprehensive and sophisticated end-to-end incident and case management process.

Risk analysis is therefore greater than solely experience and discretion from security professionals on the job, although this is a critical component. It is the culmination and the end result of an efficient and effective method of harvesting data in order to construct security solutions accordingly – leading to a fusion with the skills, knowledge and experience of security personnel into a broader framework. Our vision for intelligence-led design in security is based upon a root and branch risk management process, fed by meaningful, accurate and retrievable security intelligence.

This is not an easy vision to achieve. We see one of the key challenges in our aspiration for intelligent design as how security intelligence is fed into our processes, by our prime data capture mechanism, namely people.

Naturally, processes cannot operate without people. Similarly, processes enable people and people enable processes. In the 21st Century, the golden thread which runs between the two is the application of technology, now more so than it has ever been before. Without sufficiently enabling technology at the disposal of security providers and recipients of services, people and processes will not have the reliable high-quality access to security intelligence necessary to run an intelligent solution design process. We see this as how we surmount the challenge identified in the previous paragraphs.

In all instances, our intelligence-led design vision seeks to enable. The goal is to enable people and processes, and in doing so to make technology the corresponding enabling tool it should be. The title of this White Paper includes the term ‘technology-enabled security officers’. If people are the highly crucial one third for our three-pronged process of ‘people, process and technology’, they must have the tools with which to do the job. Again, this illustrates the totally indispensable role of technology in our intelligence-led design vision.

In our opinion, because risks do not stand still and can evolve within the blink of an eye, security solutions should evolve just as quickly.

In order to be effective they must be efficient and expedient in adapting to deal with fast-changing security risks, with a view to the prevention and mitigation of those risks through an intelligent design process.

We believe that a process of continuous improvement can help to keep security solutions up-to-date and responsive to the development and evolution of risk. Accordingly, this process will operate at its best in a cycle that deals with

incidents and the threats which they present, from incident capture through to management, investigation, mitigation and analysis, followed by measurement as to effectiveness. In short, this is an end-to-end incident and case management process fusing people, process and technology into the effective and efficient three-pronged approach outlined in this paper, as a part of our vision for intelligence-led design.

Now we will discuss how this can be made a reality via our most important commodity - namely, people.

The technology-enabled security officer

Thus far in this paper we have spoken about the 'technology-enhanced officer'. Because processes are only as good as the information fed into them people, by and large, are the prime intelligence harvesting tools (as alluded to earlier in this paper).

Gone are the days of the old-fashioned security log, and paper is rapidly becoming obsolete as a recording tool. In the 21st Century, web-accessed and cloud-based technologies are becoming increasingly the norm, with accessibility enhanced and extended by the massive expansion in capabilities via handheld devices from smart phones to PDAs, to tablets. These tools are flexible, portable and easy to use.

In our observation, the prospects for far-reaching innovation in intelligent security provision from this extensive and empowering proliferation of handheld devices, coupled with corresponding developments in software, are truly exciting for the development of the technology-enabled officer. Armed with a full suite of portable reporting mechanisms on such devices, security officers and customers alike can feed into central repositories for security intelligence. This flexibility is aided by the fact that handheld devices of these types cross the barrier between personal and professional because they are day-to-day personal gadgets as well as increasingly necessary work tools. This broadens the scope for reporting further still.

Our vision for a technology-enabled officer does not end with the officer per se; technology can and should be extended to the recipients of security services too. Intelligence gathering is not the sole preserve of the security officer, as they are reliant on a variety of sources, for example CCTV and verbal reporting of incidents and risks. However, these methods can sometimes distract the officer in the crucial moments when mitigation is required. This 'middle-man' can be cut out by technology with incidents reported by configured devices into the centralised repository we have outlined. Once in the centre, solution design can be built around analysed trends with a view to mitigation and future prevention. With vigilant eyes and ears everywhere on site(s), a rich feed of intelligence can flow into systems, thus improving security across the board.

Real time notification on a secure site, or across several, can ensure all relevant data is captured, responded to and stored for current and future solution design.

Given the nature of modern handheld devices video, audio and picture capture is possible and can be reported to the centre at rapid speed. The integration of such mobile technology, via both officer and customer, strengthens intelligence for security at the point of an incident and beyond.

Incidents and risks are as diverse as they are fast-moving. However, a sophisticated use of pattern and data analytics - via mobile technology feeding into centralised technology - can build solutions on a far more analytical level. Prevention and reduced risk exposure is a key strategic goal for this approach, in keeping with 'the prevention is better than cure' philosophy to security. This ethos feeds into our earlier reference concerning relentless continuous improvement.

Technology-enabled officers – when fused with the kind of innovations we see as the future - also have tremendous scope to enhance accountability in the provision of security services.

This approach can include, for example, proof of presence to provide reassurance to recipients of security services. Detailed and auditable data trails can limit the scope for human error by combining the distinct strengths of personnel, process and technology into a seamless package of intelligent design. They can also provide a rigorous set of benchmarks for contractual key performance indicators (KPIs).

As a further expression of accountability via technology-enabled officers, analysis of the success of mitigation tactics and deterrents can also help to shape client strategies and KPIs for the future.

Such intelligence-led design, achieved by technology-enabled officers and others, can achieve a closer realisation of the vision for ‘total’ security before, during and after security incidents.

Conclusion: Is it time?

By definition, the intelligence-led design of security solutions, based on evidence and intelligence, is more likely to be effective in prevention, mitigation and ongoing solution planning. Utilising the enormous scope of innovation provided by technology, fused with process and personnel, a forward looking approach can revolutionise how security is provided and planned for on sites.

Security officers alone will no longer be enough, and if the benefits of our vision for a 'total' approach – before, during and after – are accepted, the necessity of fusing people, process and technology will be undeniable. We see the future as equipping security personnel with the tools to make technology-enabled approaches as an inseparable part of a three-pronged process of intelligent solution design.

Data is king. Knowledge is power. Information is indispensable.

Without the ability to harvest these assets, you will not be able to benefit from them. Without the process is place, your people cannot operate to their full capacity. And, finally, without the technology to enable both, none of the above can be achieved.

Contacts

Simon Jamieson

New Product Development Manager
G4S Secure Solutions (UK)

simon.jamieson@uk.g4s.com
07711 393534

Simon has worked in a product development environment for a number of years across very diverse industries. He is an advocate of combining technology within traditional services and has a strong focus on how customers can extract the maximum value from their services, ensuring service excellence is delivered at all times.

Close to Simon's heart are ways in which G4S can develop new propositions that significantly enhance and differentiate the products and services offered to the market.

Douglas Greenwell

Strategy Director
G4S Secure Solutions (UK)

douglas.greenwell@uk.g4s.com

Originally a physics graduate, Douglas started his career at Reuters in 1991 and has worked at IBM, Dow Jones and America Express in a variety of marketing and product management roles. He joined the then Securicor Group (before the 2004 merger with Group 4 which created G4S) as Head of Product Development in 2000.

Since then, Douglas has gained overall responsibility for strategy within the business through market research, new product development and acquisitions, which has led to the launching of innovative new products. As a keen technologist, he has been instrumental in developing the company's technology strategy, including the integration of the systems business and the development and launch of a mobile product to enhance security guards.

For more information on technology-enabled security officers and intelligence-led design in security systems, please see here.