ORIENTATION GUIDE

FREEFORM DYNAMICS
Open Research and Analysis

Protective Monitoring

An Introduction to GPG 13

Jon Collins and Martin Atherton, May 2010

Protective monitoring has become important for many large organisations in the UK, as public organisations and their suppliers find themselves in a position to have to do something about it. But what does it actually involve and how can you deliver on it in a way that makes sense to your organisation?

What is protective monitoring, anyway?

CESG (Communications and Electronic Security Group) Good Practice Guide 13 (GPG 13) is increasingly being mandated for organisations involved in UK government business, including government departments, public organisations and indeed service providers and outsourcing companies.

The guide contains 136 pages and may appear somewhat daunting. However, it boils down to some pretty straightforward advice, namely: "how to protect against anything untoward happening on, or to your computer systems". For what it's worth, the lengthiness of the guide can largely be explained by its prescriptive nature.

Who or what are we protecting against? The answer is largely 'people' – who access and misuse things they shouldn't. The answer can also be 'systems'. Automated "bots", for example, can launch a denial of service attack from infected computers.

The starting point and motivation for this document is that many organisations may need to get up to speed on GPG 13 because their governing bodies have requested it, or because it has become a pre-requisite for doing business.

This document discusses the impact of GPG 13, what doing it properly enables, and offers guidance on how to treat it as part of the bigger picture of sustainable IT change, risk mitigation and business efficiency.

This paper was compiled and written on an independent basis by Freeform Dynamics, based on multiple studies during 2009-2010, within the framework of its community research programme and sponsored by Tier 3.

For more information on community research see http://www.freeformdynamics.com/services.asp.

Tier-3

Protective Monitoring as part of Information Assurance

GPG 13 has been developed by CESG as an element of its Information Assurance (IA) guidance. Here's the official line:

Protective monitoring is a set of business processes, with essential support technology, that need to be put into place in order to oversee how ICT systems are used (or abused) and to assure user accountability for their use of ICT facilities.

This merits some explanation, for a start in terms of what we are monitoring for. Not only are we talking about unauthorised access to computer systems, but also such facets as:

- Modification or destruction of valuable information
- Prevention of system or data access by unauthorised people or systems
- Fraudulent use of access or information

Note that in most organisations, the threat posed by external 'hackers' is negligible compared to the 'insider threat'. Many breaches are deliberate, of course – but some involve employees stumbling into an area where they shouldn't be looking, and taking a peek regardless (as the adage goes, "Never ascribe to malice what can be put down to stupidity"). Furthermore, some of the above can be triggered, or at least exacerbated by system failure.

Of course it would be great to simply prevent such things from happening in the first place, and you probably already have all kinds of preventative technologies in place. But what remains lacking in many organisations is the ability to oversee what's going on across the IT environment as a whole. Monitoring system use and data can be used to determine:

- Whether an attempt is being made to breach security
- What's being done and how it can be stopped
- If it's already happened, what damage was done
- Who the perpetrator was and how to locate them
- How to prevent it from happening again

From an IT perspective, while protective monitoring sounds great in principle, it may be daunting in practice due to the complexity of the IT environment as a whole, the roles and responsibilities to support it, and the specific goals you are required to achieve.

Why should you care about protective monitoring?

Given your own circumstances, you may have no choice but to implement the recommendations in GPG 13. However, a clear understanding of what you can achieve with protective monitoring should help you to implement it in a way that aligns more closely with your own organisational goals, thus helping to deliver on both.

Few organisations would deny that protective monitoring is useful, if not essential, at least in principle. However in these cash-strapped times, cost becomes a very important factor. The temptation might well be to do the minimum necessary to comply with the guidance as cheaply as possible, even if this means missing opportunities to derive broader value outside the traditional security domain.

In many organisations, protective monitoring will be just one of many initiatives jostling for budget and attention, so the case will need to be stated very clearly. The good news is, a number of benefits exist above and beyond meeting the compliance aspects. GPG 13 lists a number of these, which involve protective monitoring dovetailing with other aspects of IT security and operations:

- Risk management and situational awareness, that is, understanding how changes in context might have an impact on IT as a whole

- Reporting on performance indicators and continuous improvement, both for other compliance purposes and for more general quality assurance
- Accountability of IT use, in terms of how well services are delivered to the business
- Verification and review of protective measures, for example by demonstrating inadequacy against specific threats.

We should add 'integration with other forms of monitoring' to this list. There are strong overlaps with service monitoring, device performance monitoring, network traffic monitoring, power monitoring and so on. Ultimately, monitoring is monitoring!

Learning from forward-thinking organisations

With protective monitoring as with other strategic initiatives, we can learn from more forward thinking IT organisations which have recognised that the place to start is getting their own house in order first – running a tight ship, which is respected and trusted by the business. In service terms, it means knowing what services you are trying to deliver, provisioning them in the right way, and ensuring that services are decommissioned when no longer necessary Getting this service lifecycle right is at the heart of good IT delivery.

Leading IT organisations recognise that they cannot do everything. Businesses are too complex and rapidly changing to be understood in every detail, and indeed, neither do they need to be. Rather than trying to 'boil the ocean', ***most important is to understand the subset of things that the business does which add the most value***. If something goes wrong with these elements, the business could be at stake whether it is public or private.

From this position, protective monitoring is as much about knowing *why* one is monitoring as much as *what*, and spotting the exceptions rather than the norms. Dealing with these exceptions in an appropriate manner, with effective reporting paths, is key to protective monitoring success. From our discussions with IT decision makers, we know the difficulty is often not in implementing the technology. It is in getting the business to engage – both pre-implementation stage, or (arguably worse), post deployment when the business has to respond in some way to what's been found out.

Delivering on protective monitoring

While GPG 13 defines in detail how to approach protective monitoring for specific systems, it says little about what to do if an organisation is starting from scratch. Some clear hooks are there – for example, the first implementation principle is expressed as, "Adopt an organisation-wide Protective Monitoring strategy that defines a consistent approach and common goals". With the best will in the world, anything that needs to be done "organisation-wide" is going to be a challenge.

Rather than taking it all on at once we would suggest an approach involving the following steps:

- Decide how the principles of protective monitoring apply to your organisation
- Discover what needs to be protectively monitored
- Prioritise the systems and services which need to be dealt with first
- Isolate or remove systems that add more risk than value
- Implement monitoring capabilities as appropriate
- Implement operational roles, responsibilities and reporting

Let's look at each.

Decide how the principles of protective monitoring apply to your organisation

To start from the right place, the organisation needs first to decide the relevance of protective monitoring to its business activities. This boils down to having succinct answers to questions such as:

- What are the goals of monitoring – is it purely to achieve compliance, or does it have a broader remit?
- Who is responsible for delivering on the goals of protective monitoring, and how will success be measured?
- What general statements need to be made about protective monitoring policy, as discussed in Chapter 3 of GPG 13?
- What criteria can be used to determine whether a system, data source or user is subject to protective monitoring policy?

Discover what needs to be protectively monitored

According to Verizon's 2009 Data Breach Investigations report roughly 50% of breaches investigated in 2008 involved systems, data, connections or access rights that were unknown to the organisation at the time of the breach. To resolve this challenge, it is important to undertake some kind of discovery exercise so you can determine exactly what needs to be in the scope of protective monitoring.

Add to this that many attacks occur indirectly – that is, using some kind of intermediary system or resource – and it becomes clear that the dependencies between systems are as important as the systems themselves. For protective monitoring to be effective, you will need as complete as accurate a picture as possible of your IT environment.

Prioritise the systems and services which need to be dealt with first

Following the discovery exercise, you need to gain a clear understanding of where to prioritise efforts. An assessment could include analysis of the following three criteria:

- Risk – the 'probability-times-impact' model of risk gives a firm starting point to refine which systems and resources need to be kept in scope.
- System state – not all systems will be operating in an optimal state when it comes to security. Quite recently for example, a security vendor told us that when they reviewed their own infrastructure, they found a single firewall operating with no fewer than 22,000 rules!
- Information class – the information being handled by a given system may determine how important the system is to the business, and therefore the potential impact of a breach.

We do not under-estimate the complexity behind these criteria. However, markers such as these can provide the basis for prioritisation, using a model such as a traffic light system or similar.

Isolate or remove systems that add more risk than value

Sometimes, the best way to mitigate a risk is to remove the cause. It is not hard to appreciate the link between this line of thinking and broader activities such as infrastructure consolidation.

If a system is removed from service, it will not need to be monitored – and perhaps nor will systems that connect(ed) to it. This stage also provides an opportunity to revisit the IT architecture as a whole in the context of security – for example to ensure that any weaknesses are addressed before monitoring is implemented.

Implement monitoring capabilities as appropriate

It is unlikely that GPG 13 cannot be implemented without deploying certain technologies. If you carry out an objective and pragmatic assessment before taking the plunge, at least you will know you are spending money in the right places, and you will also have a far better understanding of other existing capabilities. The basic requirements to meet are:

- Capture and collate alerts at a system level
- Analyse event information and isolate malicious events
- Enable diagnosis of root causes

Equally, the technologies that feed protective monitoring – for example event/log management and other information correlation capabilities – need also to be selected, sourced and configured. Many organisations will have capabilities already in place, either for protective monitoring or more broadly, for service monitoring and management. A gap analysis is therefore an important element of this stage, to avoid duplication and identify candidates for upgrade or replacement.

As a final point, we would re-emphasise the importance of thinking architecturally – that is, deploying a technology platform that is flexible and scalable enough to deal with new regulations so that you don't have to re-architect it a couple of years down the line.

Implement operational roles, responsibilities and reporting

Operationally, protective monitoring requires that a number of roles and responsibilities be in place, all of which is documented adequately in GPG 13 Chapter 5. As an adjunct, do remember that the computer systems and information flows around protective monitoring are also subject to abuse, and should be treated with as much respect as other systems.

As with any implementation process, it is important that protective monitoring is considered with the future in mind as well as the present. If treated as a one-shot operation, it may come in a bit cheaper in the short term, but at the expense of longer term value. You can consider sustainability from a number of perspectives – not only in terms of operational management and ongoing support but also the tools themselves, whose own effectiveness may diminish over time.

Conclusion, Tips and Tricks

It stands to reason that protective monitoring should be considered in the context of your own business, your customer needs, your IT environment, the information it contains and the control you need to have in place. Put simply, ***protective monitoring should very much be seen as an integral element of what you do as opposed to something you have****,* or just need to comply with.

However, while it is a non-trivial undertaking, it does not need to be seen as a monolithic, expensive initiative. It also offers a prime opportunity to revisit your IT and operational environment and consider how well suited it is to your needs. Considering protective monitoring in this context could actually enable you to reduce costs as well as improve the service levels associated with existing software applications.

Alternatively, if compliance is your only goal then make sure you approach it with eyes open and for the right reasons. For example, you may have already fulfilled the majority of requirements, or because you have no other choice.

Finally, it is important to acknowledge that neither the threat landscape, nor technology are going to stand still. While nobody has a crystal ball, you should be able to understand the trajectory that legislation is taking for your own organisation. Meanwhile, deployment of new capabilities and delivery models such as virtualisation, software as a service and so on will mean that protective monitoring remains a moving target.

By adopting protective monitoring in the spirit described here, it is hoped that you will find a sustainable approach which suits the needs of the regulation *and* the needs of your business.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in ITC strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.

About Tier-3

Tier-3 Pty Ltd is a software development business with offices in Australia, UK and Japan. It has a history of technological innovation in the development of next generation computer network security solutions. The Huntsman threat management suite incorporates its patented ***Behavioural Analysis,*** a real time threat detection and integrated risk management capability.

Huntsman's unique risk based priority system greatly simplifies the burden of compliance by continuously reporting and highlighting any non-conformity to operational standards, security policies or regulatory obligations. Using patented techniques Huntsman® systematically analyses massive volumes of information to provide a continuous early warning system that alerts when things are not operating as they should.

For further information please visit www.tier-3.com.