Getting started with security metrics

by Gary Hinson and Krag Brotby

Introduction

Especially if you are new to the game, implementing information security metrics for your organization can be a daunting prospect, surely one of the toughest challenges facing any CISO (Chief Information Security Officer) or ISM (Information Security Manager). Don't feel awkward if you lack experience in this area. Few professional courses and qualifications in our field even mention security metrics. The metrics books are overwhelming[1], while the metrics advice in both traditional and social media is confusing, sometimes contradictory, and often seems irrelevant and impracticable.

---

[1] We know, we know! We did our level best to make PRAGMATIC Security Metrics both readable and usable, while fellow authors such as Andrew Jaquith, Douglas Hubbard, Caroline Wong and Lance Hayden have expressed differing but valid perspectives and offered valuable advice.

To be honest, it's daunting for us too, despite having been through the process several times already and written books on it! We have however learned the value of a structured approach, which this article explains.

The starting point

See if this rings true for you …

Perhaps the most common situation we come across in the course of our consultancy work is that the client organization has gradually accumulated a loosely-defined collection of security-related metrics through an obscure process over an unknown period. With differing opinions on what 'security metric' means, and seldom an actual list or catalog of security metrics, it's hard even to work out what security metrics there are. Furthermore, they almost certainly haven't been selected or designed as a coherent suite, but have evolved piecemeal.

Security metrics are typically not an integral, core part of the organization's management, despite the need for measurement being noted in standards such as ISO/IEC 27001. The woeful situation in information security contrasts markedly with other, more established forms of management such as financial management for instance. You can be quite sure that when someone says the company is 'managed by numbers', they are not talking about its information security metrics!

In many organizations, certain security metrics circulate for no better reason than that various security systems/applications churn out the numbers by default, and someone has naively assumed they must therefore be worthwhile. Almost invariably, there is no clear *a priori* business purpose or demand for them, although some may end up finding uses, and by happy coincidence some of those uses may actually be valuable!

We refer to these as 'coffee table metrics', akin to so many glossy nature photography books and celebrity gossip magazines.

Generally speaking, at this stage of immaturity, the organization's security metrics are so sub-optimal that it would barely matter if they were stopped … which in fact is one way to find out if any of them are earning their keep. A brave CISO or ISM might quietly stop circulating the least impressive metrics and wait to see what happens next. If nobody even *notices*, that's a pretty clear sign that they were

merely red tape. If anyone complains that the metrics are 'late', it's worth asking why that matters, digging deeper to discover how they are actually being used. If the complainant normally repackages and forwards the numbers to someone else, adding little value in the process, let the delay continue: there's a fair chance the numbers will not be missed.

On a more positive note, the fact that you are reading this article and obviously have an interest in security metrics is a very good sign. Also, launching from such a low base means your early gains will be impressive once you make a start on improving your security metrics, which leads-in to the next - and arguably the most important – part of this article.

Defining and stimulating the demand for security metrics

You probably appreciate that, although you and/or your colleagues may feel that your security metrics are poor and ought to be improved, it is far from clear what 'improve' means in this context. As well as the nagging doubts about where they end up, there is often a lack of direction and purpose for the existing security metrics. Resolving that conundrum is what this paper is all about.

Please, whatever else you do, don't automatically assume that more security metrics are The Answer. In metrics, less is more, paradoxically. The sheer number of metrics correlates very poorly with their utility and value. Choose quality over quantity, every single time.

The approach we recommend is a back-to-basics rethink about your security metrics. If that sounds scary, bear with us as we gently lead you through the steps.

Determine the business purposes for your security metrics

Why are security metrics needed? What will they achieve for the business? What use will they be? What is their value proposition? Key to answering questions of this nature about your security metrics is first to understand the business purposes for information security, raising a parallel set of questions. Why is information security needed? What does it achieve? What use is it? How does it generate value?

You might jabber on about information security being about protecting information, ensuring its confidentiality, integrity, availability, ensuring compliance with privacy and other obligations, and all that jazz – which is fine as far as it goes but is completely generic and not very helpful. For metrics purposes, you need to get more specific. What is the point of information security *for your organization*? What information deserves protection? What is it being protected against? What might be the business consequences if it were compromised in some way? How important, valuable and vulnerable is information relative to other corporate assets, such as buildings and people?

For us, information security boils down to risk management … but that too raises tricky questions. What risks are of concern in relation to information? How do information risks compare against the risks to other assets? Hold that thought for now – we'll pick up on it later.

Working backwards from all those questions, you need to elaborate the business drivers for information security, which gets us to the vital message of this article: **security metrics help you direct and control information security to mitigate business risks that management finds unacceptable for the business.** Trust us: knowing what drives the business to secure its information makes a world of difference.

OK, but how?

Determine the business imperatives for information security

Developing a coherent suite of information security metrics involves systematically addressing a set of rhetorical questions.

1. What is the organization's true purpose?

If you believe that particular question is answered by the dreaded 'mission statement' plastered so prominently on the office wall or the corporate website, you are sadly mistaken. The mission and values posters leave off much more than they say. Worse still, the version that appears in print has invariably been word-smithed almost beyond recognition for political, motivational and

It could for instance be argued that Microsoft is not a computer company after all. Its purpose in life is not actually IT. Microsoft's core strength is *marketing* IT, painting its business activities in a different light.

marketing purposes. It is a vacuous and contemptible piece of puffery, despite what management might implore you, and your customers, to think.

2. What are the organization's objectives?

The mission or rather the purpose of the organization may be its ultimate objective, but usually there are other/interim objectives, waypoints that it intends to secure on the way to stardom, and perhaps tarpits that it intends to avoid. What are the objectives that will enable the organization to achieve its mission? As with the corporate mission statement, documented business objectives only tell you part of the story. You need to spend time with senior management exploring and getting to the bottom of the objectives. Tease out the cunning wrinkles that a competent management team will have invented to give the organization its edge, its competitive advantage: they may well be entirely undocumented due to their sensitivity, so even if there is next to no evidence of information security being an explicit part of the objectives, at least you know management cares about securing some of its business information!

3. What are the organization's business strategies?

Senior managers are difficult to get hold of. They are invariably busy, often preoccupied, and may be reluctant to discuss sensitive business matters with you in any detail, especially if you are way down the hierarchy (it might help to explain why you need to know this stuff, what the information will enable you to do, emphasizing that you can be trusted to keep confidential matters confidential!). Business strategies may be more accessible and will help you fill-in the gaps. Senior and middle managers generally know about the business strategies because they tend to be involved with developing and executing them. The best way for you to find out what the business is really doing is to spend time speaking with the relevant managers, having already made the effort to obtain and read whatever strategic information is available in writing.

If you have successfully completed steps 1 and 2, step 3 will flow naturally. With a solid understanding of senior management's high level goals and objectives for the organization, the strategies will make more sense and you will ask more sensible, insightful questions.

4. What are the organization's risks and opportunities?

Although shown as a separate step, you will probably have started pondering the information security risks already during the previous 3 steps. Besides those relating to information, there are risks and opportunities in the commercial, market, financial, compliance, personnel, technical, political and other spheres. It's important to get a perspective across all of them in order to support a balanced portfolio of risk (*e.g.* particular information security risks that concern you may barely register with senior management if they are dealing with, say, a serious possibility of a major loss arising from adverse exchange rate movements). This is where risk management professionals come into their own, so spend some time with your risk manager/s to gain that sense of perspective.

5. What is the organization trying to achieve through information security?

The organization's goals and objectives for information security should be pretty clear by now. You should be able to express them quite eloquently *in business terms* – an important point that will pay dividends in due course. Your job in step 5 is to blend your professional knowledge and expertise in information security with the understanding and insight you have gained into the organization's strategic directions. Elaborate on the information security risks *and* opportunities (*e.g.* aside from defending the organization's information assets, it may be appropriate to go on the offensive in some situations, perhaps actively exploiting weaknesses in a competitor's information security or pushing compliance to the limit). You should now be in a position to develop or update and refine the organization's information security strategy and plans, maybe drafting a business case to invest in an information security management system or putting plans in place to support the information security aspects of various business initiatives and projects.

6. What security metrics are needed?

At last you're ready to get down to brass tacks, shortlisting information security metrics that are necessary to support all the concerns, decisions and activities arising from the previous 5 steps.

We find it helpful to think in terms of three distinct types of metrics:

1) **Strategic security metrics** – these are measures concerning the information security elements of high level business goals, objectives and strategies. For example, if the organization needs to bolster its information security capabilities and competences in order to support various business initiatives, without expanding the budget, metrics concerning the efficiency and effectiveness of information security are probably relevant. Broad-brush metrics relating to information security risks, capabilities and value tend to exist at this high level. The reporting period may be one or more years.

Provided you haven't cut too many corners, several strategic and management-level metrics should flow naturally from your understanding of the business imperatives for information security. Others may not be so obvious, so you may need to think creatively. See chapter 5 of PRAGMATIC Security Metrics for further sources of inspiration.

2) **Security management metrics** – there are numerous facets to managing information security risks that could be measured, hence many possible metrics. We recommend making a special effort to identify management metrics that directly relate to achieving specific business objectives for information security, supplementing those that are needed to manage the information security department, function or team just like any other part of the business (*e.g.* expenditure against budget). Management-level metrics tend to be reported/updated on a monthly or quarterly basis. Metrics concerning information security projects/initiatives (*e.g.* implementing dual-factor authentication) and the information security management system (*e.g.* security incident statistics) are typical examples.

3) **Operational security metrics** – at the lowest level of analysis, most information security controls, systems and processes need to be measured in order to operate and control them. Metrics supporting security operations are normally only of direct concern to those managing and performing security activities. They include both technical and nontechnical security metrics that are often updated on a weekly, daily or hourly basis. They are unlikely to be of much interest or value beyond the information security and related technical functions, although some

provide raw data for management-level metrics (*e.g.* plotting the number and severity of information security incidents reported and resolved each day or week will indicate the trends over a longer timespan that may prompt changes in the way incidents are handled).

It should not be hard to relate every single metric seriously under consideration – even the more obscure and detailed ones – in some way to the business imperatives securing information. Being able to express things in business terms is a massive payback for all that hard work in previous steps. It means that the metrics are **R**elevant and **M**eaningful to the organization, which hints at the final step ...

7. Which metrics are **PRAGMATIC**?

Since there are so many information security things that could/should be measured, and so many different ways to measure them, your shortlist of potential security metrics may be quite lengthy. This is exactly the situation for which the **PRAGMATIC** method was invented. The method, described at length in our book **PRAGMATIC** Security Metrics, involves evaluating and scoring each metric under consideration using nine criteria represented by the **PRAGMATIC** acronym:

Predictiveness: metrics that tell you something about what is likely to happen, *before* it happens, in good time to do something about it, are more use than those that are purely historical. Metrics that generate clear, reliable trends score strongly on this criterion.

Relevance: irrelevant metrics are distracting and unhelpful. Relevance refers to *both* information security *and* the organization's business.

Actionability: there's not much point in reporting stuff that the audience can do nothing about! Furthermore, good metrics provide information in a format that guides the response in terms of its direction *and* scale (not just telling us "We are off-track", but off which way and how far).

Genuinness: metrics that can easily be fabricated or manipulated lack credibility and impact, especially if the reporters have a vested interest in the numbers. It may be literally impossible to eliminate biases and game-playing, but some metrics are better or worse than others.

Meaninfulness: implicitly understanding what the numbers means, and more importantly how they relate to the business objectives, makes good metrics resonate with and motivate the intended audience. Conversely, "clever" metrics that have to be explained laboriously and repeatedly are not earning their keep, and may even lead to inappropriate responses due to misunderstandings.

Accuracy: this criterion reflects the value of proportional control. Binary values (such as compliant or non-compliant) may appear clear-cut but can be misleading (being trivially, marginally or briefly non-compliant means something quite different to being flagrantly and outrageously non-compliant).

The scores generated by the PRAGMATIC method make it simple to rank the shortlisted metrics and select the ones that will simply be adopted or at least piloted. Furthermore, the method can often be used to improve individual metrics by addressing the factors that limit their scores.

Timeliness: if it takes too long to gather, analyze and report something, its predictive value is degraded to the extent that the indicated response may be inappropriate by the time it is taken. Timeliness can be a tough challenge in the more dynamic, fast-paced aspects of information security such as malware, frauds and hacks, where we are struggling to keep pace with the threats.

Independence: generally speaking, numbers that have been, or could be, independently verified by a trustworthy, impartial advisor (such as the auditors) carry more weight than those based on unverifiable or purely subjective information. This criterion reflects the integrity of the data and the measurement process.

Cost-effectiveness: the ninth criterion concerns the net value of the metric, not purely the cost. Surveys, for instance, are a relatively expensive measurement technique but a well-designed survey puts hard numbers on soft issues that are otherwise extremely difficult to measure and hence manage. This criterion is a final reminder that good information security metrics have a business purpose and don't exist purely for their own sake. To put that another way, *not* using **PRAGMATIC** security metrics could be a costly mistake.

Conclusion

We are sorry to disappoint you if you were hoping for a simple checklist to follow, or a set of recommended security metrics. We make no bones about it: security metrics are hard to get right, not least because every organization is unique. We have laid out a process you can follow to select and design a suite of information security metrics that will prove valuable for your particular organization, whatever its nature, size and industry. Our parting message is once again to emphasize being business-focused. Get this right and your security metrics will become an essential tool that management could not envisage going without.

Additional reading

Brotby, Krag (2009), "Information Security Governance", Wiley.

Brotby, Krag (2009), "Information Security Management Metrics", CRC Press/Auerbach.

Brotby, Krag and Hinson, Gary (2013), "PRAGMATIC Security Metrics", CRC Press/Auerbach.

Hayden, Lance (2010), "IT Security Metrics", McGraw Hill.

Hubbard, Douglas (2010), "How to Measure Anything", Wiley, 2nd edition.

ISO/IEC 27004 (2009), "Information Security Management - Measurement".

Jaquith, Andrew (2007), "Security Metrics", Addison Wesley.

Wong, Caroline (2012), "Security Metrics – A Beginner's Guide", McGraw Hill.

About the authors

Dr **Gary Hinson** PhD MBA CISSP has worked in IT system and network administration, information security and IT auditing since the 1980s, consulting since 2000. His day job involves preparing materials for NoticeBored (NoticeBored.com), an innovative security awareness subscription service. He is also responsible for ISO27001security.com supporting the global community of ISO27k users. Gary was originally a scientist researching bacterial genetics.

Krag Brotby CISM CGEIT has 30 years' experience in enterprise computer security architecture, governance, risk, and metrics. He is the principal author/editor of ISACA's Certified Information Security Manager Review Manual, plus a number of books and articles. Krag has served on ISACA committees and the California High Tech Task Force Steering Committee, and frequently presents conference workshops, seminars and courses in metrics, governance-risk-compliance (GRC) and risk. Krag holds a foundation patent for digital rights management.