nCircle

Top 10 Tangible Measures for Effective Security Risk Management

Table of Contents

> "Metrics provide the **essential focus and prioritization** to determine precisely where to apply security effort. Organizations that exploit metrics to shape their security initiatives have **fewer incidents, compliance failures and lower cost operations**."
>
> -David Lacey

1. Introduction

"You can't manage what you can't measure" is a frequently cited quote, usually attributed to W. Edwards Deming. It is not completely true and it's not precisely what he said[1]. Because the truth is that there are many things in life which simply cannot be known or measured. The important point, however, is that you can't manage a business process effectively and efficiently without reliable intelligence of costs and events. The point that Deming actually made is that it is fatal to rely on the visible figures alone. You have to probe below the water level of the iceberg to understand what is really happening. Nowhere is this more important than in security risk management, because of the invisible nature of many of the most dangerous threats, exposures and events. Sometimes this is by deliberate design: espionage and fraud, for example, are intended to be covert, untraceable activities. But it is also because of the silent and unseen nature of electronic transactions, which cannot be observed without the aid of a suitable software monitoring device.

Visibility and metrics are the foundations of security risk management. Visibility of threats, vulnerabilities, breaches and incidents is fundamental to identifying, assessing and mitigating the associated risks. Monitoring of customer communications, user behavior and the status of essential controls are increasingly necessary to satisfy regulatory compliance requirements. Metrics also provide the basis for sound, mature process management. Readers familiar with capability maturity models[2] will recognize the vital role of measurement in achieving the higher levels that reflect best industry practice and advanced process performance. Those familiar with balanced scorecards will appreciate the importance of measurement in achieving business goals. Managers who have to submit business cases to support their spending plans, will understand the need for quantifiable evidence of security costs and benefits.

Metrics provide the essential focus and prioritization to determine precisely where to apply security effort. Organizations that exploit metrics to shape their security initiatives have fewer incidents, compliance failures and lower cost operations[3]. Metrics underpin the development of mature, effective governance processes by enabling management to 'close the loop' on policies and standards, i.e. to check that the controls required have been implemented and are actually working, consistent with the 'Plan, Do, Check, Act' philosophy of the classic Deming Cycle (see Figure 1), which is fundamental to achieving continuous process improvement.

---

[1] The point Deming made was more subtle. He stated that "running a company on visible figures alone" is one of the seven deadly diseases of management. By this he acknowledged that some of the most important figures you need might in fact be unknown or unknowable.

[2] Such as the Carnegie Mellon Software Engineering Institute Capability Maturity Model, an advanced application of the process management concepts of Total Quality Management, drawing on ideas developed by Crosby, Deming, Juran and Humphries.

[3] An example is the British Royal Mail Group who substantially reduced their incident levels and security operating costs through the analysis of metrics on incidents and vulnerabilities.

Figure 1 – The Deming Cycle of 'Plan, Do, Check, Act'
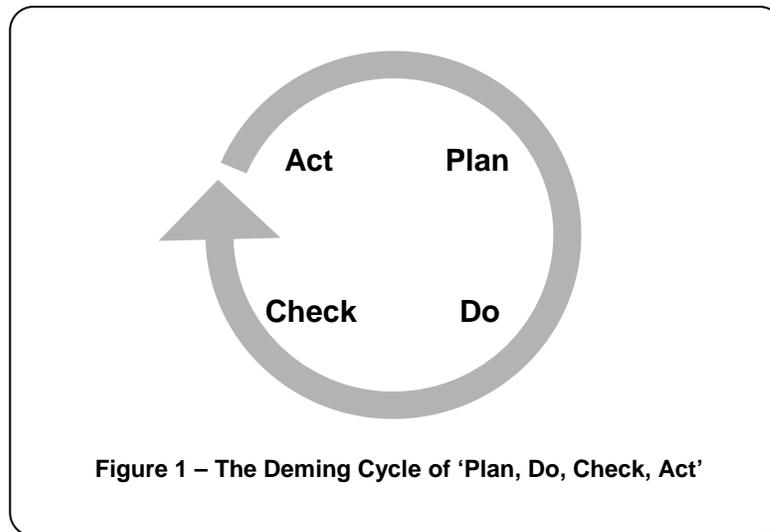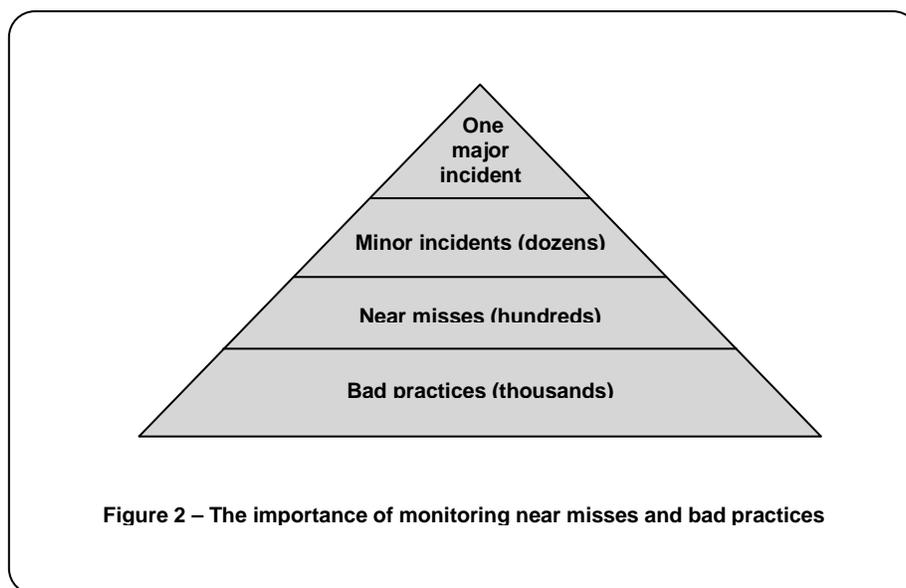
2. Sources of Inspiration for Useful Metrics

As Deming indicated, not all information is knowable but the trap is to only rely on the data that comes to you as a side effect from other business processes. An effective metrics system must be designed, implemented, tested and refined. It must also align with business objectives (company scorecards for example), IT strategy and security strategy and architecture. In fact the starting point in the process of selecting your metrics should be to identify the overarching business goals that shape the organization's short and long term focus. Further considerations would then include the need to support regulatory compliance requirements and any longer-term strategies developed for IT, security or risk management purposes. Typical questions that should be asked when designing a metrics system would include the following:

- What are the organization's **business goals** and what metrics will be used to help indicate whether or not these goals are being met? Is there a balanced scorecard? Business goals are likely to include objectives such as cost reduction, service quality improvement, business expansion, revenue protection or innovation. Relevant risk management metrics might be measures that indicate trends in operating costs, service outages, customer problems or the time required to carry out essential risk processes that underpin organizational or product changes.

- What regulatory **compliance requirements** does the organization have to meet and what metrics can be identified to support these? Examples of useful security and risk management metrics might include the level of compliance of individual systems and platforms against internal security policies and established industry standards, the impact and probability scores assigned to identified security risks or the number of outstanding audit actions. In the financial sector, Basel II requires historical incident data to support operational risk assessments. In the retail sector, the PCI Data Security Standard[4] requires third party verification of regular network vulnerability scanning.

- What are the **supporting strategies** of the IT, security and risk management functions? Typical strategies might include outsourcing, IT portfolio management, service quality,

---

[4] Compliance with the Payment Card Industry (PCI) Data Security Standard is required for merchants who process large numbers of credit card transactions.

identity management or de-perimeterization[5]. Supporting metrics for such strategies might be ones that provide an indication of the accuracy of the IT asset register, the risk profiles of major applications, the levels of incidents that impact services, or the vulnerability of platforms supporting critical applications and processes.

- What metrics are required to enable efficient **prioritization of effort**? Risk mitigation initiatives need to be ordered according to the risk profile of the organization and infrastructure. This is especially true for vulnerability management initiatives which need to give priority to the highest risk and most critical platforms for immediate remediation. Examples of metrics that can help support this process would be those that indicate the business criticality of a platform and its relative vulnerability to a potential breach, based on vulnerability scores and the overall network topology.

- What metrics can support **prevention of incidents**? To understand this better, it is useful to draw and analogy with safety. Security incidents are likely to follow a similar pattern to safety incidents. Classic research by Heinrich (1936) showed that on average, corresponding to every major incident, there are 29 minor incidents and 300 near misses, and probably thousands of individual bad practices that led to the incident. Metrics that identify dangerous practices or near misses are a powerful tool for avoiding damaging future incidents. See Figure 2 below.

One major incident

Minor incidents (dozens)

Near misses (hundreds)

Bad practices (thousands)

Figure 2 – The importance of monitoring near misses and bad practices

- What metrics can support **process improvement**? All processes offer potential for continuous improvement and metrics play a key part in setting and monitoring performance goals. For security and risk management processes, useful metrics include the cost and time taken to carry out essential security activities such as risk assessments, incident investigations, patch management or reviews of systems or infrastructure. In addition, having clear ownership and reporting on network security performance will create a culture of continuous improvement.

---

[5] De-perimeterization is defined by the Jericho Forum (www.jerichoforum.org) as 'The act of applying organizational and technical design changes to enable collaboration and commerce beyond the constraints of existing perimeters, through cross-organizational processes, services, security standards and assurance'.

3. Achieving High Performance and Process Maturity through Metrics

Management systems and processes can be differentiated by their maturity, their effectiveness and their performance, three characteristics that are closely correlated. Models developed by Carnegie Mellon Software Engineering Institute to measure process maturity indicate that high-performing processes are ones that are well-defined, measured and capable of continuous improvement. Such processes have lower operating costs, faster execution times and produce higher quality deliverables. They also have more predictable costs and timings based on historical data. Mature processes exploit technology that is fit for purpose, cost effective and easy to use. Achieving the higher levels of process maturity requires a cycle of continuous improvement. At the heart of this approach is the exploitation of metrics to correct deficiencies and achieve continuous performance improvements. Progressive improvements using metrics are more effective than large scale, once-off changes because they are easier for the organization to digest and carry less risk of failure. Figure 3 illustrates the steps of a typical maturity model for Information Risk Management[6]. The higher levels demand a highly disciplined approach to measurement.
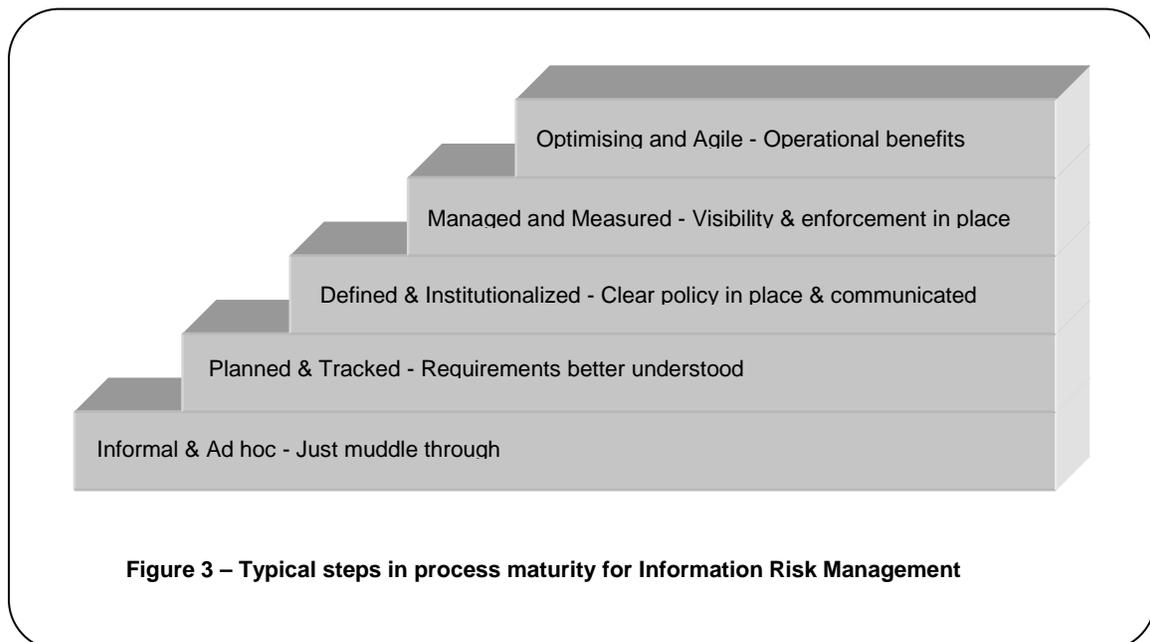
Optimising and Agile - Operational benefits

Managed and Measured - Visibility & enforcement in place

Defined & Institutionalized - Clear policy in place & communicated

Planned & Tracked - Requirements better understood

Informal & Ad hoc - Just muddle through

Figure 3 – Typical steps in process maturity for Information Risk Management

---

[6] This illustration is based on a new model developed by the author for Chronicle Solutions.

4. What Can and Can't be Measured

Not all things are measurable or knowable, and the cost of measuring some items can turn out to be prohibitive. We cannot know how many attacks have been deterred by good security. We cannot design foolproof measures of human capabilities. We cannot measure the vulnerability of IT platforms without specialist technology. But it is surprising what can be achieved with a little imagination and a modest budget. Simple techniques have been developed by organizations and used effectively to reduce incident levels, lower operating costs and even assess the general security attitudes and behaviour of staff.[7] New technology is continually emerging to enable automated detection, assessment and monitoring of equipment attached to corporate networks. The following table sets out some ideas on the useful and practical metrics that can be implemented without excessive spending on process changes or technology.

Objective	Metrics that can be used
Vulnerability management	Number of vulnerabilities identified on platforms
	Number of outstanding patches for a given set of platforms
	Time taken to apply and verify effectiveness of patches to a percentage of platforms
Incident reduction	Number of incidents reported to the Helpdesk in a given period
	Ratio of actual virus incidents to those blocked at email gateways
	Losses of laptops and mobile phones in a given period
	Numbers and types of investigations in progress
Service improvement	Number and length of outages over a given period
	Number of customer problems reported over a given time
Prioritization of effort	Measures of business criticality for applications and supporting platforms or asset values by host or network
	Percentage of IP assets under consistent security management
Cost reduction	Number of password resets at the Helpdesk[8]
	Time taken to conduct risk assessments and reviews
Risk mitigation	Risk scores (impact x probability) for a given set of risks
	Number of outstanding remediation actions on a given system
Improving staff behaviour	Questionnaire-based measures of knowledge, attitudes and behaviour
	Network ownership identified with security performance routinely reported

---

[7] The Royal Dutch/Shell Group designed an effective questionnaire in the early 1990s to measure user knowledge, attitude and behavior regarding information security.

[8] Password resets can be a surprisingly high cost, generally amounting to well over 10% of the overall Helpdesk traffic and potentially costing millions of dollars for large organizations.

Compliance	Percentage of ISO 17799 controls implemented for a particular system, service or organizational unit
	Number of outstanding audit actions
	Percentage of automation controls used for internal security and regulatory policy compliance

5. Priorities for Selecting Metrics

Most of the preceding examples of metrics will be valuable to any security risk function. Enterprise-wide metrics systems, however, cannot be easily implemented overnight. Many require time and effort to design, agree, specify, implement, test and debug[9]. The sensible approach is to build a metrics system over time, progressively adding new measures and refining the accuracy, presentation and analysis of existing ones. With this approach, priorities have to be assigned to metrics to ensure that the most vital ones are implemented first. Metrics that meet the following criteria should be considered as high priority:

- Required to help prevent a potential immediate attack

- Essential to support a regulatory compliance audit

- Needed to support a critical security or risk management activity[10]

---

[9] For example, adding extra questions and fields to a Helpdesk process involves software changes, process changes, training and testing.
[10] Such as prioritization of the application of critical software patches to platforms.

6. Top 10 Measures for Effective Risk Management

Of all the events, issues and indicators that can be physically and technically measured, the following items are judged to be the best, contemporary measures for effective security risk management. As with many measures, this one is subjective - based on experience. It should be taken as a starting point, rather than a definitive list, for organizations aiming to establish an enterprise-wide metrics system.

Top 10 Measurement	Why it is important
1. Trend of number of critical vulnerabilities on Internet-facing platforms	Vital to provide the necessary visibility to safeguard the frontline infrastructure from immediate attack
2. Time taken to apply and verify critical security patches to business critical platforms	Needs to be monitored carefully to ensure it keeps up with the shrinking window between vulnerability announcements and the release of exploit code
3. Percentage of IP network under continuous management with relative business criticality of platforms and workstations	Essential to prioritize the application of patches and virus updates, and also any remediation work following a widespread virus/worm outbreak
4. Current risk scores (impact x probability) for the Top 10 risks	Required for compliance purposes and also to focus attention and effort on the highest areas of risk
5. Number of outstanding audit actions not fully implemented	Essential for compliance purposes, provides an early indication of a potential audit failure
6. Number of outstanding remediation actions on the most critical business application systems	Needed to provide visibility of the compliance status and vulnerability of the systems that support critical business operations
7. Exceptions to password and access control policy in a given period	Can be a major expense as well as a risk for organizations and might also highlight potential system design problems or the need for additional user/customer education
8. Exceptions to internal security policy by device, network group or business	Policy and configuration control and reporting are critical to a risk-based approach and understanding position in relation to compliance requirements
9. Amount of down time through incidents and failures to critical business services over a given period	Can indicate potential security issues as well as quality of service problems
10. Time required to conduct risk assessments for major business improvement initiatives	Provides an indication of the efficiency of the risk management process and its potential impact on major projects and business agility

7. The Role of Technology in Achieving Visibility and Measurement

Technology is necessary to shine a light on otherwise invisible electronic events. It can also help to probe below the surface of the iceberg and identify, assess, filter and consolidate previously hidden characteristics of systems, platforms, communications and user behaviour in real time. New security technologies such as nCircle's agentless security risk and compliance management solutions[11] are emerging and evolving to help the security risk management function gain enterprise-wide visibility of emerging threats, and mitigate them before a major incident is caused. They also deliver the essential information required to enable continuous process improvements and the evidence needed to demonstrate compliance with legal and regulatory requirements.

8. Summary

Visibility and measurement are the very heart of security risk management. Without them it would be impossible to identify, assess and mitigate risks. They are also the key to effective process management. Identifying appropriate metrics ideally requires a consideration of the organization's business goals, strategies and compliance requirements, and the measures that could be used to prioritize activities and help prevent incidents. Safety provides a useful analogy on how incidents can be prevented by monitoring near misses and correcting bad operating practices. Smart use of metrics, especially when coupled with powerful technology, underpins the development of effective governance processes by enabling management to 'close the loop' on policies and standards and apply continuous process improvements. Although not everything is measurable or knowable, with a little imagination and a modest budget suitable metrics can always be identified. Enterprise-wide metrics systems, however, cannot be implemented overnight. They need to be developed over time, progressively adding new measures and refining existing ones. Priorities need to be assigned to ensure that the most vital metrics are implemented first. Metrics that help prevent potential attacks, support compliance audits or are needed to support a critical activity, should take priority. This paper presents a Top 10 list of the most important metrics in order to give organizations a head start in the design of their enterprise metrics system.

About the Author

David Lacey is a leading international authority on Information Security Management with more than 20 years professional experience, most recently as Director of Information Security and Risk Management for the Royal Mail Group. Prior to that, he was responsible for Information Security policy and standards for the Royal Dutch/Shell Group. Before that he was Head of IT Security for the British Foreign & Commonwealth Office. David is a keen futurist and innovator, firmly believing that the best way to predict the future is to invent it. Amongst other things, David played a major role in the development of the British Standard BS7799 and the design of the associated certification schemes. He is a regular keynote speaker at international conferences and has served on numerous professional Boards concerned with Information Security and Compliance, including the APACS Security Advisory Group, the BCS Security Forum, the Jericho Forum (which he founded) and the UK National Identity Card Private Sector User Group (which he chaired). David is also a joint founder of the Institute for Information Security Professionals (IISP) and is the first Honorary Fellow of The Jericho Forum.

---

[11] nCircle is the leading provider of agentless security risk and compliance management solutions, see www.ncircle.com for more information.

About nCircle

nCircle is the leading provider of automated security and compliance auditing solutions. More than 4,000 enterprises, government agencies and service providers around the world rely on nCircle's proactive solutions to manage and reduce security risk and achieve compliance on their networks. nCircle has won numerous awards for growth, innovation, customer satisfaction and technology leadership. nCircle is headquartered in San Francisco, CA, with regional offices throughout the United States and in London and Toronto. Additional information about nCircle is available at www.ncircle.com.

nCircle

nCircle, Inc.
101 Second Street
Suite 400
San Francisco, CA 94105 USA
+1 415 625 5900
www.ncircle.com
email: info@ncircle.com