GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

An Introduction to Information Security performance measurement
Using Balanced Scorecards for measuring IS performance.

José Carlos Faial
November 4, 2002
Assignment version 1.4b

Abstract
After the deployment of security systems and devices like firewalls, rolling out updates, patches and implementing security policies, IS managers are discovering that the evaluation of their efforts is not an easy thing to do. Information Security is an area where good measures and methodologies for performance and success evaluation still missing. In this document I'll show how the concept of *Balanced Scorecards (BSC)* that has been used by financial and general business managers since it was developed by Kaplan and Norton some years ago, can be used to evaluate IS performance. I'll also, discuss some problems on evaluating IS performance and propose a generic scorecard.

Introduction to scorecards
Before Kaplan and Norton have introduced the concept of scorecards as a tool for measuring performance, most companies were using only traditional measures like "profit and losses" as a way to improve business and define strategy. Kaplan and Norton's idea is that those traditional measures should be supplemented by using other measures: customer satisfaction, internal processes and ability to innovate. These additional perspectives should assure future financial results. For each perspective, they have proposed three components: mission (e.g. be the largest Application Service Provider in Latin America), objectives (e.g. provide our customers with high quality services and products) and measures (e.g. new customers, renewed contracts). The framework of the BSC methodology consists of translating and linking each perspective into corresponding metrics and measures for each situation, as different markets, product strategies and business units require different scorecards to fit their mission, strategy, technology and culture. On this way, many researches have been working on BSC concept applied to IT, and a generic IT scorecard were proposed consisting of four perspectives:

- Business contribution
- User orientation
- Operational excellence
- Future orientation

As explained, this scorecard differs from the corporate business scorecard because it's a departmental scorecard, so the metrics and measures as well mission and objectives should be changed to match the IT's position and objectives inside the company and its contribution to the business.

© SANS Institute 2000 - 2005 Author retains full rights.

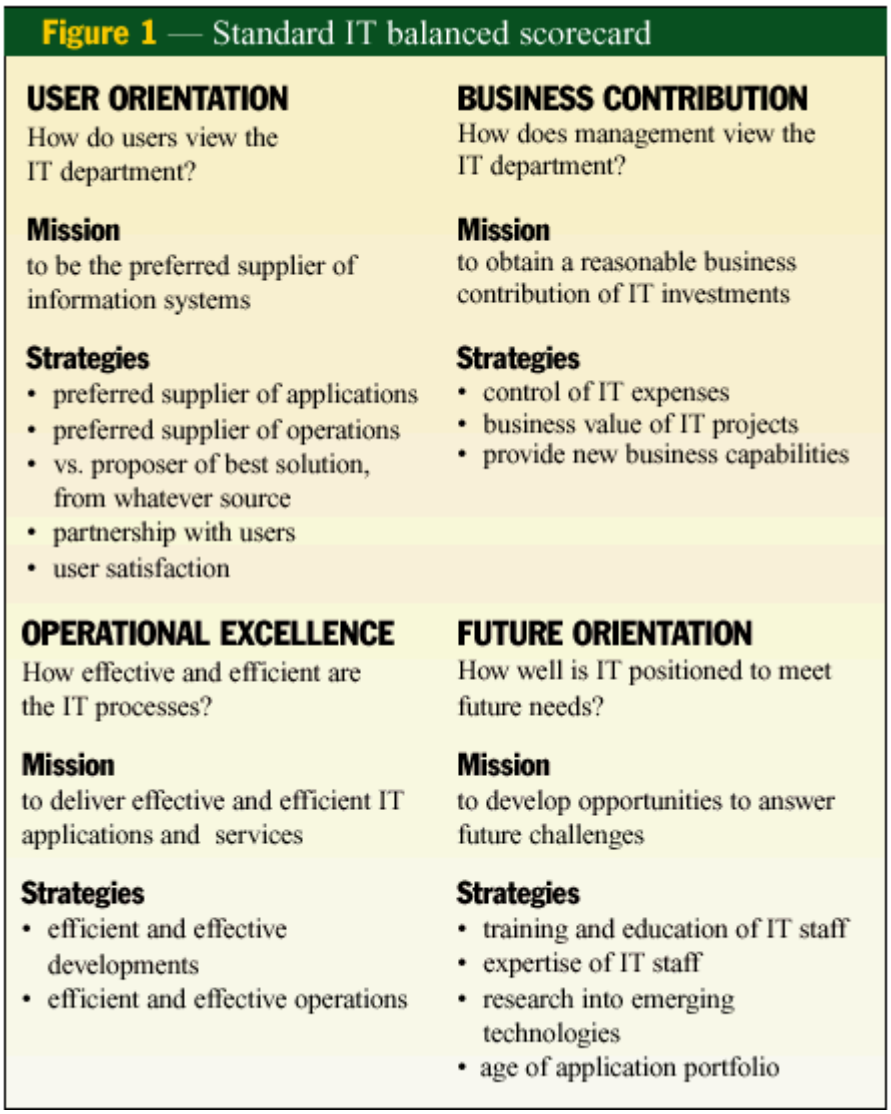


Figure 1 – Standard IT scorecard © IT Governance Institute

The cause-and-effect relationships between these perspectives are given in figure 2. All scorecards must have a clear definition of those relationships as well a good mix of measures (outcome measure and key performance indicators).

© SANS Institute 2000 - 2005 Author retains full rights.

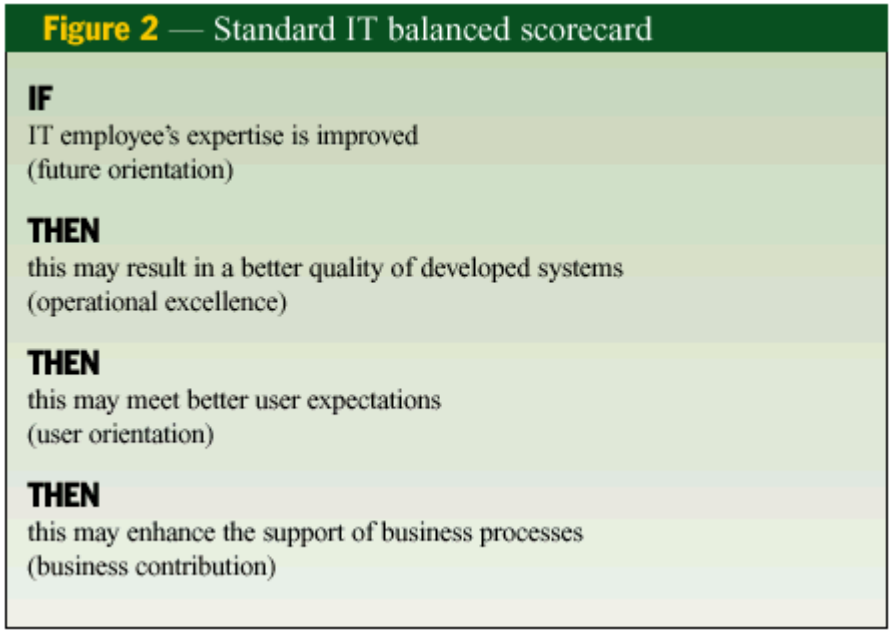


Figure 2 – Cause-and-effect relationships between scorecard perspectives[4] © IT Governance Institute

As IT is becoming a crucial part of the business and not only a simple "computer department", the need for secure business e-transactions and mechanisms for sharing information securely growths at an increasing rate. Because that, Information Security Managers are challenged every day with questions like:

- Which project should be our highest priority to improve our security?
- Are the investments with users security awareness training succeeding?
- Is the firewall adequately handling our traffic needs?
- Is the Intrusion Detection System working as desired?
- Are the Information Security Policies adequately implemented in a way to allow IT and other areas to drive their business while reducing security incidents?
- Are we prepared to handle new security threats, responding in a quickly, effective and efficient way?

Many of these questions can be answered with the help of scorecards. The hardest challenging on using it in Information Security is the selection of the right metrics and measures.

Information Security

In recent years, Information Security has crossed the IT department frontiers and reached business and support areas like human resources department. Information Security is no more a single matter of IT Security, it's now a critical success factor for the whole company, because companies are discovering that Information is one of its more valuable asset, and like every physical asset, it must be protected. In the Information Age, the company that has the right information in the right time will succeed against its competitors.
The BSI/ISO-17799 standard states:

© SANS Institute 2000 - 2005 Author retains full rights.

> Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

And defines Information Security as:

> Preservation of confidentiality, integrity and availability of information.

For these reasons, Information Security is a huge subject. Starting from the Systems and Network Security, trough Physical Security of the perimeter, Disaster Recovery procedures, Social Engineering protection, to Business Continuity Planning, users training and education and many others, all driven by Security Policies and adhering to laws and legislations (e.g. HIPAA). It will be impossible if I try to summarize all necessary activities to play the role of Information Security and correspondent metrics to evaluate it in a few pages, so I'll focus on Computer Security, not going so deeply into other areas.

Computer Security

There are many definitions for Computer Security. The NIST (National Institute of Standards and Technology) defines Computer Security as:

> The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

This is a generally accepted definition for Computer Security. From these definitions, we can formulate a general mission for Computer Security:

Mission

"Protect automated information system resources in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities".

The main objectives can be also derived from the definitions above (with some pluses!):

Objectives

- Ensure the integrity, confidentiality and availability of automated information resources.
- Minimize security incidents.
- Support business requirements.
- Optimize costs.

© SANS Institute 2000 - 2005 Author retains full rights.

- Minimize risks.
- Obtain security certifications for systems and personnel.
- Improve efficiency and effectiveness.
- Educate users.

Metrics vs. Measures
To understand the differences between metrics and measures I'll adopt the definition given by Mr. George Jelen of International Systems Security Engineering Association:

> Measurement is a one-time view of specific parameters represented by numbers, weights or binary statements. Metrics are produced by taking measurements over time and comparing two or more with a predefined baseline.

Challenges on Measuring Computer Security
It is not so difficult to define the objectives of Computer Security, however it's not clear what should be done do achieve it nor how to measure if we have really achieved it. Why? To answer this question we'll take a look at some issues pointed in two workshops about this subject, one held by NIST, Approaches to Security Metrics and other by Applied Computer Security Associates (ACSA) and The MITRE Corporation, Workshop on Information Security System Scoring and Ranking:

- Security means different things for different people
- Lack of standards
- Lack of benchmarks and baselines
- Ambiguity
- Immature discipline
- Different values placed on Information Security Metrics by Governmental (policy driven) and Commercial (profit driven) sectors.
- Technology changes

According to the results of those workshops, the above issues are the main responsible for the problems in measuring IS performance. To give a real-world example of the results of these problems, lets look at a report from The Office of Management and Budgeting:

> Is the Federal government spending enough on IT security? Nearly sixty percent of the Federal agencies reported spending between 2.1 and 5.6% of their total IT investment on security. Five agencies reported spending between 7.3 and 17% and five reported between 1.0 and 2.0%. OMB assessed the agencies' security performance against the amount they spent on IT security and did not find that increased security spending equals increased security performance. Therefore, at this point, there is no evidence that poor security

© SANS Institute 2000 - 2005 Author retains full rights.

is a result of lack of money.

This conclusion was based on executive reports sent from US Government Agencies with guidance from OMB and questionnaires issued by NIST as the above document states. However, is clear that without a standard for measuring IS (Information Security) performance, companies and government agencies will issue results based on different approaches and different metrics, resulting in inaccurate values. That is supposed to be happened in the above example I guess.
So, if managers are going to answer the question "Is the money invested in security resulting in a proportional protection?" they must have proper tools and methodologies to measure and compare the results. The scorecards methodology is a great tool to do it, however the measures and performance factors to be used should be well defined to avoid interpretation errors and to provide alignment with the control objectives defined by management. For example, if a IS Manager have defined "70% successful virus infection reduction" as an objective and measured the "# of successfully virus detected (unsuccessfully infections)" it is not clear if the objective were reached without correlating the measures:

Table 1 - Statistics of anti-virus system

Period	# of users	# of new viruses in the wild for the period	# of successfully infections	# of unsuccessfully infections
2001	310	120*	80	1100
2002	40	90*	5	230

* not real value, just an example.

Based on above table, is the IS Manager's objective accomplished? Yes, if we look at "# of successfully infections" only, however if we correlate all the measures, taking in consideration the reduced number of employees (less targets) for 2002:

2001: 80/310 = 0.25 infections/users
2002: 5/40 = 0.12 infections/users
Reduction Target (70% of the 2001 baseline) = 0.07 infections/users
Real Reduction = 2001 – 2002 = 0.13 infections/users
GAP = 0.06 infections/users

We conclude that there is a GAP of 6% percent to accomplish the desired result. What can we conclude from the other measures? Can we evaluate the real performance of the anti-virus system by looking at them? Which other metrics should we be using in order to get a full picture of the anti-virus performance? Also, we must take in consideration the environment where the system is running (a system connected to Internet is much more exposed to new viruses than others – high risk) and the technologies used (personal anti-virus, anti-virus gateways…). We are challenged by problems like these when defining good metrics. The solution for this problem is: to measure the performance of your Information Security project, the control objectives and

© SANS Institute 2000 - 2005 Author retains full rights.

metrics should be defined in a way that they can be easily correlated one which other. When defining an objective, managers should also define which measures must be evaluated to bring the proper results. This brings us another question: Witch Computer Security measures should be used? There is no universal standard for selecting security measures, this is one of the big problems on measuring IS performance. Each company should select a set of measures that best fits their own objectives. However, some work was already been done for standardization:

- The Common Criteria
- FIPS 140-2 (for crypto modules)
- TCSEC (Orange Book)
- SSE-CMM (this one presents everything you'll need to define and evaluate your measures and metrics)

All of above are good examples of well-defined standards that can be used as a source for measures when evaluating IS performance. In the other hand, a lot of work has been done to provide management with good guidelines on defining IS control objectives, critical success factors and audit steps: the COBIT framework issued by ISACA is one example. The COBIT is being accepted as an industry standard for IT and IS control objectives and IT Governance framework. Standards are important because they can guide evaluators in the same direction when measuring IS performance trough companies, thus acquiring more accurate results. However, whichever is the standard to be chosen, it must take in consideration all aspects of the Information Security: people, processes, policy and technology. For this reason, COBIT is the best resource available as a source for guidelines on defining control objectives, critical success factors and key performance indicators for managing IS.

Examples of IS performance measures
Below are some IS measures examples:

People
% of employees trained in basic security awareness program
% of employees trained in Security Policy
# of risk incident reports issued by employees (if people are reporting, its because they are concerned about security, thus the security awareness training is succeeding)
# of registered incidents caused by employees (not externals) (this is an indicator that the Security Policy training should be reviewed, reformulated or even remade from scratch)
% of SANS GSEC certified systems administrators

Technology
% of hardened Windows servers following Center for Internet Security benchmark level 1
# of intrusion attempts detected by IDS

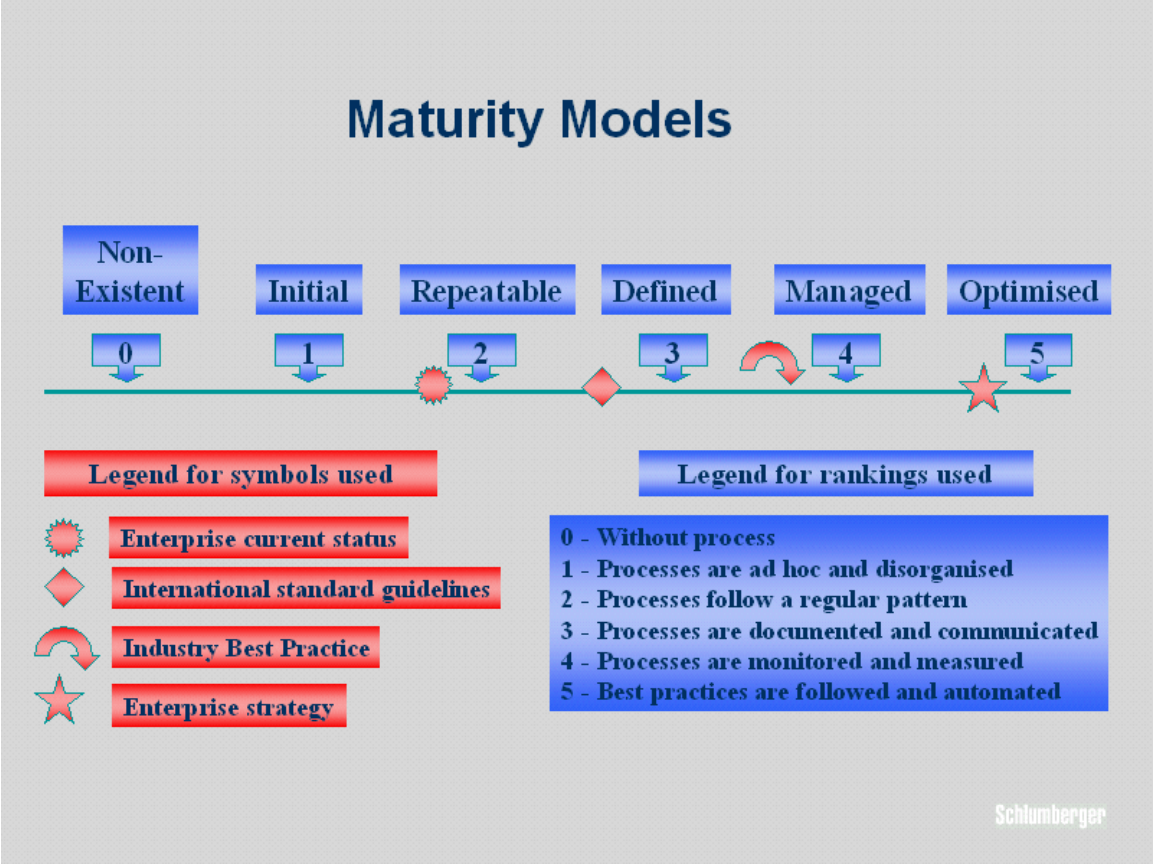
© SANS Institute 2000 - 2005 Author retains full rights.

% of false positives issued by IDS (it should be as low as possible)
# of blocked connections at border firewall vs. % of legitimate connections blocked (this can show you that your firewall is blocking legitimate connections. Too bad! It can be measured by looking at complaints from users or customers trough email, helpdesk and etc)
# of successfully systems compromises

Policy
% of systems in compliance with access control standards
% of users that have read and signed the Information Security Policy

Processes
Maturity degree of adoption of the processes
% of projects delivered on time (this show you that the processes are efficient)
% of projects delivered on budget (this show you that the processes are effective)

How to measure
Depending on the type of the metric chosen, a different tool for performing the measurement should be used. For example, to evaluate how a process is being used at the company, a measurement tool called Maturity Model can be used:



© SANS Institute 2000 - 2005 Author retains full rights.

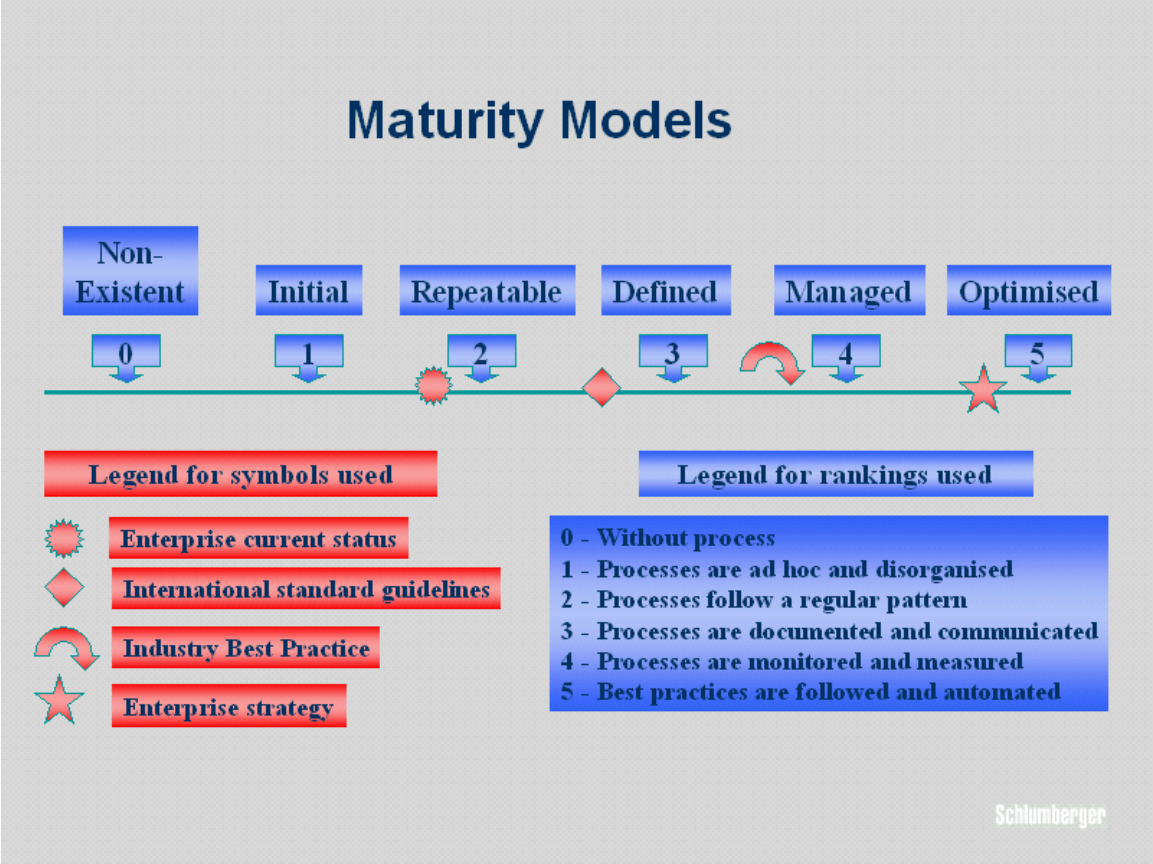


Figure 3 – Generic Maturity Model

The Maturity Model is an easy to understand scale, where organizations can set their objectives and compare with actual results. Those results can be collected trough audits, questionnaires or interviews. This technique is based on Capability Maturity Model (CMM) methodology. Besides Maturity Models, most of the work can be done looking at systems logs and collecting statistics. Another well accepted measurement methodology to evaluate the strength of the company's computer security is the Penetration Tests and Vulnerability Analysis, also called pen-tests. The objective of a pen-test is to break into company's network and systems and collect evidences of the successfully break-in while assessing vulnerabilities. Generally, experienced security consultants with hacking skills perform the pen-tests. The vulnerability analysis can be done with the help of automated scanning tools like Nessus, Internet Security Scanner, Nmap, SAINT and others. The pen-test and vulnerability analysis reports can be used as a good measure, but this technique has some problems:

- Sometimes pen-tests cannot be repeatable, so no values to compare with previous pen-tests will be available
- Technology changes every time, a predefined baseline maybe not be valid in the next year
- Skills of the security consultant that is performing the pen-test. High

© SANS Institute 2000 - 2005 Author retains full rights.

skilled consultants can break more easily into the system than a less experienced one. If successive pen-tests are being performed by inexperienced auditors, this can give a false sense of improvements in security.

Building a Scorecard to evaluate Computer Security

In the next paragraphs I'll develop a generic scorecard to illustrate how this tool can be used to evaluate computer security. I'll not try to develop a scorecard to cover all aspects of computer security nor I'll look at all possible metrics and measures. My objective is to give some examples to serve as a foundation of a more complete work on this subject. In reality, the companies should develop their own security scorecards, as they have different objectives in computer security.

As explained before, the scorecard's approach is to split the analysis in different perspectives, each one with its own mission and objectives (or strategies). On developing a scorecard for computer security we must ask "What are the perspectives that give a better overview of the computer security and its contribution to the business?". There is no single answer for this question, but I can try to figure out some perspectives that may be used with some success, looking at the six main activities necessary to play the IS role, as stated by International Guidelines for Managing Risk of Information and Communications Statement #1: *Managing Security of Information*, issued by the International Federation of Accountants. Lets see it in the next page.

According with this guideline, to play the IS role six main activities are necessary:

- Policy Development and improvement
- Roles and Responsibilities
- Design and Planning
- Implementation
- Monitoring and Correcting
- Awareness and Education

The graphic in the next page show how these activities relate to each other.

Develop Security
Policy
Define Roles and
Responsibilities
Design (Planning)
Monitoring and
Correcting
Training and
Education

Acting
Acting
Acting
Acting
Feedbacking

© SANS Institute 2000 - 2005 Author retains full rights.

Implementing

Acting

These activities, relate to each other as follow:

Figure 4 – IS role main activities

However, I truly believe that a good Information Security Police must take care of the definition of roles and responsibilities as an integral part of the policy, thus reducing the main activities to five. This is a generic framework for the IS activities, a better (and updated) approach is shown in the next picture:

Develop Security
Policy
Design (Planning)
Monitoring and
Correcting
Learning

Acting
Acting
Acting
Feedbacking

Implementing

Acting
Processes
Training
Focus on Process
Focus on People
Focus on Technology
Focus on Policy

Figure 5 – IS role main activities updated

This updated framework is clearer to understand, as the relationships between IS activities and IS perspectives (policy, technology, process and people) are better defined. Process must exist and be followed in all tasks of IS management (acting and feed backing); training must be given to all users and IS team members while developing or updating the policy, as well when design, implementing and monitoring the systems (IS and IT team members). The contribution to the business is dependent (and a result) of the success of this framework. To measure if it is succeeding, the following perspectives are proposed:

- Future orientation (people): represents the human and technology resources that IS will need in order to drive its services and to be prepared to handle future threats.

© SANS Institute 2000 - 2005 Author retains full rights.

- Operational excellence (process): represents the process, actions and methodologies employed by IS to deliver its services and to manage its infrastructure and systems.
- Systems orientation (technology): represents the results of the actions taken to minimize the risks of security vulnerabilities of the computers and network systems.
- Business Contribution (policy): represents the value given to the business by security projects and initiatives like development of a security policy.

Is important to note that (look at figure 5) the Business Contribution is a result of the entire framework, which starts and is dependent of the Security Policy. So, the contribution to the business is directly proportional to the success of the security policy. This is the relationship between the Information Security Policy and Business Contribution.

Table 3, in the next page, shows the proposed Computer Security Balanced Scorecard. In the following table we see how they relate:

Cause-and-effect relationship of IS scorecard
IF IS employee's staff skills are improved and users properly educated (Future orientation) **THEN** This may result in people ready to implement, adopt and follow new technologies and procedures (Operational excellence) **THEN** This may result in better improvements in the overall security of systems and network (Systems Orientation) **THEN** This may enhance the support of business relying on IT (Business Orientation)

Table 2 – Cause-and-effect relationship

SYSTEMS ORIENTATION	**BUSINESS CONTRIBUTION**
What are our success in protecting our computers systems and networks against threats while keeping it available for our customers?	Are the Security Policy and the actions taken to implement it proportioning a significant return of the investments?

© SANS Institute ins full rights.

compromises will show us that the number of detected vulnerabilities still high enough to allow hackers to succeed. In reality, a really good attacker will need just one single hole to get into your systems! For our lucky many of them are not so good.

The second objective is “improve monitoring”, that means “look more closely at your systems”. We can have a picture if our monitoring systems are succeeding looking for detected intrusion attempts and comparing it with the false positives rate. A high rate of false positives means that you need to fine tuning your monitoring systems. The data necessary to do this evaluation can be collected from your NIDS and/or HIDS sensors deployed around your network and/or by collecting security events from your logs by using tools like Swatch. Catch and stop SPAM should be a important activity of monitoring systems as well, so I’ve listed some points to measure if its succeeding. The data can be collect from the tools you may have implemented. Sendmail will report that over syslog if properly configured (see also the Realtime Blackhole List, it’s great!).

Detect unauthorized access is one of the most important task any monitoring systems must perform, because that don’t forget to look if your systems is really alerting for this kind of issues. At finish, the most polemic activity of monitoring systems, detect misuse. For some companies misuse can be interpreted as a management problem, for others it’s a security problem as important information resources are being wasted with, for example, browsing web for fun. If misuse is in your Security Policy, it must be handled as a security incident and must be detected and stopped. Reports from your HTTP proxy can help you on detecting unrelated to work sites being accessed; a simple file search trough you file server can help you find for .mp3 files and so on.

Block malicious code is critical in the Internet age. If you don’t have any updated anti-virus software running, disconnect your Internet link now! By malicious code I mean any piece of software like virus, Trojans, worms or other plagues. Look at then carefully.

The next objective is “enforce correct usage”. This is directly related to misuse, although we are now measuring if we are properly blocking it. I propose you to look for the number of unauthorized files (like music) detected. If this number is rising over time, training and policy communication must be reinforced. Another important system to enforce correct use is the email infrastructure and web surfing. There are a lot of reports in the Internet talking about employees wasting time and bandwidth with emails and web sites visits not related to work. If you have any blocking rule active, look if they are being triggered. Examples of blocking rules are “block outgoing mail if bigger than XX megabytes” or “block incoming mail if it contains XYZ world in the body of the message”. Lots of software to perform email blocking is available in the market, and most e-mail servers comes with a limited set of features to block or deny email. To block web sites, you’ll need a URL filter device like Websense, or a proxy server that has this capability. SQUID, a free web proxy, has some nice URL blocking features.

© SANS Institute 2000 - 2005 Author retains full rights.

The last objective of this perspective in the proposed scorecard is “keep systems available”. While there are a lot of discussion on the availability subject about who is the responsible for the availability of the systems (is it an IS or IT operations problem?), we all must agree that IS has at least to guarantee that all critical information systems have redundancy mechanisms and protection against DoS attacks. I’ll not enter into discussion if systems performance monitoring and capacity planning is a responsibility of IS staff or not, although ISO-17799 states that it should be in your security policy, so IS must at least enforce that this occurs. Whatever are the redundancy and DoS protection mechanisms you have in place, we measure if they are succeeding or not looking at how many percent of time your systems were up and available for users. Course, 100% of availability is impossible in practice, but many Service Level Agreements requires a minimum of 99% or 99,9% of time. The value of “Unavailability time of critical infrastructure and business systems” must be as less as possible (this is a “negative” measure). Some evaluators would prefer to always work with “positives” measures, i.e., higher the value the better (its clearer to understand). So, you can replace that measure with, for example, “% of time critical systems were available”. In practice, it’s the same thing.

Measures for Operational Excellence

The Operational Excellence is concerned with quality of work, if necessary actions and methodology employed to deliver or reach the objectives were done and if the processes of IS are effective and efficient.

Measures for Operational Excellence
Deliver projects on time % of projects delivered on time # of new IT implementations delayed by security concerns
Deliver projects on budget % of projects delivered on budget % of projects delivered below budget
Quickly response to incidents % of network being monitored by NIDS % of servers being monitored by HIDS % of generated logs being centralized and automatically analyzed % of systems with automatic alerting mechanisms in place % of systems with an incident response planning Avg. time spent to detect the incident Avg. time spent to respond to the incident
Improve systems hardening Avg. time between the release date of patches by vendors and its local deployment Avg. time used to test a patch in the lab environment Avg. time spent to deploy patches on critical systems after tests are concluded % of hardened Windows 2000 servers following Center for Internet Security benchmark level 1

© SANS Institute ins full rights.

are to handle it (have you tested your disaster recovery procedures recently?).

Prevention is the best way to avoid incidents and the best way to do prevention is hardening our systems (and people, but I'll discuss this later). Most incidents can be avoided if we keep our systems updated, so we must evaluate the effectiveness of our processes on doing it. Although, we know patches are not enough if the systems are not securely configured. To help us on this, The Center for Internet Security works on development of "Consensus Benchmarks", a set of documents and tools to improve the security of Operating Systems, routers, firewalls and other systems. The benchmarks provide directions on hardening the systems, like services to disable and registry settings to modify, minimum patch level and etc. There are benchmarks available for operating systems like Linux, Solaris, HP-UX and others. I've listed a measure to check what percentage of our Windows 2000 servers meets the CIS Benchmark, but I could have listed other benchmarks as well.

Periodic audits must be performed in a regular basis. We must pay close attention if they are being performed with the desired frequency. Remember that the results of the audit (pen-test, vulnerability assessment and etc.) are assessed by Systems Orientation perspective.

The measures of "% of critical information and infrastructure systems with automatic availability monitoring" and "% of critical information and infrastructure systems with high-availability mechanisms" will give us a snapshot on how resilient our critical information systems are and if we are looking at them.

Measures for Business Contribution
The Business Contribution of Information Security is the main objective of our performance evaluation. It reflects the success of our Security Policy and efforts to implement it.

Measures for Business Contribution
Minimize security incidents causing public embarrassment # of computer security incidents causing public embarrassment Money lost by computer security incidents Money saved with prevention, detection and proper reaction
Support new business initiatives # of new IT implementations delayed by security concerns
Policy Communication % of security policies and plans communicated to stakeholders
Provide business continuity Number of critical business computer systems that have adequate continuity plans

We start our evaluation looking at the most important thing we must assure to get new customers and keep the old ones: the company's public image. Incidents always happen and a single one may be enough to destroy years of good reputation of a company. So, we must look closely to them and put a rate

© SANS Institute ins full rights.

demand. If an IT initiative is being delayed by security concerns, it's an indicative that something is wrong with our security capabilities. This will have a great impact over business, so we must pay attention if this is happening.

To support business that relies on computer systems, IS must ensure that the critical components of this IT systems have a proper continuity plan in place. The measure of critical computer systems that have a continuity plan must be as higher as possible.

Measures for Future Orientation
In Information Security, people always come first. We are generally pointed as the weakest link in the security process. Because that, IS must work hard to improve security awareness of users and expertise of its security personnel. Below is the proposed scorecard for this perspective:

Measures for Future Orientation
Professional Certification for systems administrators and IS staff % of IT personnel SANS GSEC certified % of IS staff with advanced SANS GIAC certifications
Keep users informed on security policy % of users that have read and signed the security policy
Educate users on security awareness % of users that have received security awareness training Avg. security awareness exam grade # of risk incident reports issued by employees # of registered incidents caused by employees
Maintain IT and IS personnel informed about security advisories and announcements % of IT and IS personnel receiving CERT advisories % of IT and IS personnel joined bugtraq mailing list % of vendors' security announcing mailing list we have already signed for
Keep IT and IS personnel updated on new technologies, threats, vulnerabilities and trends % of IT and IS personnel that have received training last quarter % of IS personnel attending to SANS conferences last year Use of the research lab

Security is a continuous and hard job, for this reason people directly involved with this subject must be well trained. However, security is an everyone responsibility, so we cannot forget of the users. They must receive special and effective training. Recently, the NIST have released a draft paper called "Building an Information Technology Security Awareness and Training Program" that will help you in the proper direction of development of your own training strategy if don't have one (and for sure it will help you improve any existent program).

© SANS Institute ins full rights.

new security advisories and announcements (this will also reflect in the patch update process) and giving IS personnel regular quality training. And don't forget to give your folks someplace to practice what they have recently learned. A research lab is essential to develop practical skills. Take a look if it has been used frequently.

Conclusions

It's a hard thing to do, but it's possible. Measure IS performance can be done with the help of proper planning and good methodologies. If you want to compare with other companies you must follow some standard, otherwise you can develop your own set of measures and metrics that best fits in your own security objectives.

The proposed scorecard is an example of the use of BSC tool. Of course this is an introductory paper that doesn't go deeply in details of this wonderful tool. As you get involved with scorecards you'll note that the bests ones are those simple with a few number of (very) objective measures. But, that is the big challenge we have in IS performance measurement: to choice the least number of measures that will give us the greatest overview of IS performance. Although, some evaluators, like myself, prefer to look at the details.

Audience is also an important thing: please, don't give your Board of Directors measures about false intrusion positive rates! They will not even understand what you are talking about. The above scorecard best fits in the audience of an IS manager.

Look at some nice references below. They will show you how to use the results you've collected to help you on deciding which projects should have priority over others to give will better results in the next measure, among other nice things.

Final note

At the time I was writing this document, the NIST have released a draft on the subject of Information Security performance evaluation. The document "Draft NIST Special Publication 800-55, Security Metrics Guide for Information Technology Systems" contains detailed information on building an effective security performance evaluation program. Unfortunately, I didn't take my hands on this document on time to use it as a reference for this work, however if you are serious on security performance evaluation you should consider reading this draft. Anyway, I hope this work can help someone.

References

Kaplan, R. and Norton. The balanced scorecard: translating vision into action. Reading: Harvard Business School Press, Boston, 1996b.

Van Grembergen, W. "The Balanced Scorecard and IT Governance". Information Systems Control Journal. I (2000): p. 40 (Reprint available at:

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.itgovernance.org/balscorecard.pdf)

Van Grembergen, W. and Timmerman, D. “Monitoring the IT process through the balanced scorecard,” Proceedings of the 9th Information Resources Management (IRMA) International Conference, Boston, May 1998, pp. 105-116.

British Standard. Information Security Management – Part 1: Code of practice for information security management. Reading: BS 7799-1:1999. 1999: 1-3

National Institute of Standards and Technology. “SP 800-12 An Introduction to Computer Security: The NIST Handbook”. The NIST Special Publications. October 1995. URL: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf

Kaplan, R. and Norton, D. “Using the balanced scorecard as a strategic management system”. Reading: Harvard Business Review. January-February 1996a, pp. 75-85.

Katzke, S. “Security Metrics - What Are They?". Approaches to Security Metrics Workshop. June 2000. URL: http://csrc.nist.gov/csspab/june13-15/Katzke.pdf

Applied Computer Security Association and The MITRE Corporation. “Proceedings of Workshop on Information Security System Scoring and Ranking”. May 2001.
URL:http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf

Jelen, G. “SSE-CMM Security Metrics”. June 2000. URL: http://csrc.nist.gov/csspab/june13-15/jelen.pdf

National Institute of Standards and Technology. “Approaches to security metrics”. June 2000. URL: http://csrc.nist.gov/csspab/june13-15/metrics_report.pdf

Office of Management and Budget. “FY 2001 Report to Congress on Federal Government Information Security Reform”. 2001. URL: http://www.whitehouse.gov/omb/inforeg/fy01securityactreport.pdf

National Institute of Standards and Technology. “The Common Criteria Project”. URL: http://csrc.nist.gov/cc/

National Institute of Standards and Technology. “FIPS 140-2, Security requirements for Cryptographic Modules”. June 2001. URL: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

© SANS Institute 2000 - 2005 Author retains full rights.

DoD. “Trusted Computer System Evaluation Criteria (Orange Book) ”. DoD Rainbow Series. December 1985. URL: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.pdf

International Systems Security Engineering Association (ISSEA). “SSE-CMM”. URL: http://www.sse-cmm.org

The IT Governance Institute. “The Control Objectives for Information and related Technologies (CobiT)”. URL: http://www.isaca.org/cobit.htm

International Federation of Accountants. “Managing Security of Information”. International Information Technology Guidelines. January 1998. URL: http://www.ifac.org/Store/Details.tmpl?SID=9628081811406&Cart=103642124023332

NIST. “SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems”. NIST Special Publications. September 1996. URL: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

NIST. “DRAFT Special Publication 800-50, Building an Information Technology Security Awareness and Training Program”. July 2002. URL: http://csrc.nist.gov/publications/drafts/draft800-50.pdf

© SANS Institute 2000 - 2005 Author retains full rights.