



# 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 permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

## ***Defining Policies Using Meta Rules***

Dan McGinn-Combs

March 14, 2002

Many of the available papers, books and articles written about security begin with the blanket statement that there is a need to base security decisions on policy. But what is security policy itself built on? Relatively few discussions of security policy emphasize coordinating them with business objectives. In many instances, the starting point is that there are bad guys “out there” and all the good guys are “in here.” But using this as a basis for making the decisions about what to put in a security policy is just not sufficient to describe the current business climate.

This paper seeks to initiate a discussion on how to design and implement security policies within a company. It first describes a methodology for developing security policies based on the concept of meta-rules, rules which define how to write rules. It then describes how to use measures to determine the effectiveness of the policies in a business context. Finally it shows the relationship between a measurement system and a systematic review of policy to verify and validate the meta-rules chosen as the basis for security policy.

### **The Purpose of Business**

*“The purpose of business is to create and keep a customer.” Peter Drucker*

Business involves activity targeted at particular objectives. Foremost among these objectives is the essential purpose of maximizing long-term owner value by selling goods and services. (Sternberg, 1998) The emphasis on value over profits is important. While the profit may be an important consideration, it can be subject to manipulation as has been recently witnessed in the much over-discussed collapse of Enron. In addition, an unrealistic focus on profits over value can push business management to make decisions laden with risk in an effort to reap short-term profit at the expense of long-term business health. (Riordan, 1997)

It can be argued, however, that even a focus on long-term value is insufficient to sustain a business. There is some dissent about the completeness of this definition of business. The ethical and social responsibilities of business to its community are often raised components which not only improve its value, but also increase its viability over the longer term. (Riordan, 1997) This additional component is seen in the debate over the difference between a brick-layer who is working for a daily wage and one who is building a cathedral. (Brunton, 2001)

However, this accepted definition of at least the economic function of business is sufficient for the task at hand. In summary, then, any activity which is not targeted at this core objective, the long-term owner value, is by definition unproductive and counter to the essential nature of the business.

### **The Business Purpose of Security**

As any student of the economic side of business knows, productivity is the key to being

successful. Successful business today operates in conjunction with a computer network. Computers and associated networks have been attributed with much of the successful innovation and high productivity levels experienced in business today. (Koretz, 2001) In other words, a business is as bound to its network as it is to its essential functions and in fact sometimes those essential, core functions **are** the network as the Centrata ([www.centrata.com](http://www.centrata.com)) business model shows. (Koretz, 2001) This business seeks to make use of the computer time on millions of personal computers while they run a special screen saver much like the Intel Peer-to-Peer initiative (<http://www.intel.com/cure/>) which links millions of PCs into a virtual supercomputer. The Intel initiative has already been used to help in the compute-intensive effort to find a molecule which will help cure Anthrax (Richards, 2002).

Since the business model today includes the communications made possible by a computer network, and these are the activities which have been shown to increase productivity and thereby long-term owner value, it is very important to ensure that the activities on the network are limited to those which support the business of the company. Achieving this goal is security.

### **Policies in Implementing Security**

Policies are the bedrock of a secure network design and the primary mechanism for defining the boundaries for those activities which on the one hand support and on the other hand do not deter the business. Therefore the purpose of a policy is to elicit behavior which is designed to conform to business goals and to exclude behavior which detracts from business goals. In other words, the purpose of policy is to drive business-related and business-focused behavior into an organization while displacing non-business related (and by definition, unproductive) behavior.

### **The use of *Meta-Rules* to define rules of behavior**

In the real world, the meta-rules, or rules which govern how to make rules, determine the real dollar costs in implementation of a change, and therefore the pace of economic growth. Security is generally regarded by business as promoting a static state of affairs, that is one in which change occurs rarely, if ever. The perceived impact of security at best is that it stifles economic growth and at worst it detracts resources from the needs of the business (Hart, 2001). Carefully and consciously designed security meta-rules, however, can both facilitate security and maintain the economic or business growth necessary to sustain a business. Therefore meta-rules should be designed in such a way as to clearly define which behaviors properly support both the core business activities and permit changes which foster growth in productivity. (Schreiner, 2001)

### *Design of Meta-Rules*

A rule which does not have a meta-rule ancestor will likely suffer one of two fates. It can become ossified, rigid and unchangeable. In this circumstance, it will not be able to meet new needs and differing circumstances. Without the strength of a meta-rule, a rule may also become subject to changes based not on the business requirements, but on the bargaining power of those seeking the change. Changes which then occur will be abrupt and cause disruptions within the economic framework of the business instead of smooth

growth. Any changes imposed this way will more likely be based on whim or fashion rather than on thoughtful design and may even be implemented too late to keep the business from self-destruction. (Schreiner, 2001)

In most real-world cases, meta-rules are neither explicit nor carefully designed. Therefore, the basis for making policy decisions becomes more fluid and subject to impulse, desire and negotiation skills. However, when meta-rules are explicitly defined, it becomes a relatively simple matter to determine which policies may conform to the meta-rules and which do not.

Below are the design criteria for meta-rules (Schreiner, 2001).

- At the end of a meta-rule chain, there must be either an unchangeable rule or a meta-rule that acts on itself.
- Irreversible decisions should be more difficult to approve than reversible decisions.
- The weight given to a request for a meta-rule change corresponds to the weight of the long-term value of that change.

### **Internet Security Policy Using Meta Rules**

*“Business, more than any other occupation, is a continual dealing with the future; it is a continual calculation, an instinctive exercise in foresight.” Henry R. Luce*

#### *Objective*

The purpose of Internet Security is

1. To permit the business to operate unhindered by external interruptions,
2. To permit required business communications via the Internet,
3. To limit activity to those required by the business, and
4. To identify and respond to disruptions or attempted disruptions of business.

#### *Policy Statement*

The following meta-rules govern the design of rules which are implemented as policies on network monitoring systems, Internet routers and firewalls in order to achieve the objectives.

1. There is an INTERNAL network, surrounded by a perimeter consisting of firewalls.
2. IP addresses internal to this perimeter are not outside.
3. Initiation of a well-defined connection from internal to external is permitted.
4. Initiation of any connection from external to internal is forbidden.
5. Internet services are provided on a network (called DMZ) which is, by definition, external.
6. Hiding or masking internal configurations (including IP address) is part of securing the internal networks.
7. Each rule and each combination of rules must be simple and understandable.
8. Inbound connections are permitted only to employees, who must be authenticated

- and the traffic must be encrypted.
9. Traffic entering the INTERNAL network is examined for suspicious activity.
  10. Traffic leaving the INTERNAL network is monitored.

### *Definitions*

1. Well defined: consisting of Telnet, FTP, http and https.
2. Encryption: using IPSec, ESP, PFS, MD5
3. Authentication: using SecureID




































The *Objective* section comprises the unchanging or self-modifying rules. These rules would only change if the business itself changed. In the extreme case, one of these rules might change or even be removed if the business requirements no longer justified it. For example, the “ability to identify and respond to disruptions” may some day no longer be important to the business.

These rules should flow from *Objective* to *Policy Statement* to *Definitions*, each building upon the other in a chain of meta-rules. The *Definitions* section can change independently from the *Policy Statement* and yet remain in compliance with the *Policy Statements*. The *Policy Statements* might change, to permit for example inbound connections from authenticated Vendors and yet remain in compliance with the *Objective*.

### **Expressing Policy Based on Meta-Rules**

Once the business’ *Objectives*, *Policy Statements* and *Definitions* are identified, the policy must be expressed as a series of rules which can be enforced at the network level. This will typically take place on a firewall. To be clear, a policy is not a series of rules, but a “plan or course of action.” (Riverside, 1988)

Firewalls generally form the primary means of enforcing policy. They do this by implementing a series of rules each of which should conform to the overall policy. Each rule describes a network activity and associates an action for that activity. As network packets traverse the firewall, each is compared to the list of rules to determine which activity is being attempted. At the first matching rule, the action, *drop*, *encrypt*, *reject* or *accept*, is executed (Checkpoint, January 2000, page 272). The policy forms the guide on which the decision of which action to choose is based. One must be able to trace each rule in the rulebase back to the *Definitions*, *Statement of Policy* and the *Objectives* or the rule is not in compliance with the meta-rules.







No.	Source	Destination	Service	Action	Track	Install On	Time
1	 Any	 Firewall	 Any	 drop	 Long	 Gateways	 Any
2	 Local-Network	 Any	 telnet	 accept	 Long	 Gateways	 Any
3	 Local-Network	 Any	 http	 accept	 Long	 Gateways	 Lunch
4	 Any	 Web-Server	 http	 User Auth	 Long	 Gateways	 Any
5	 Any	 Any	 Any	 drop	 Long	 Gateways	 Any

The rulebase shown above is a simple set of firewall rules which conform to the meta-rules defined earlier. The first rule, Rule 1, is designed to hide the firewall from normal network activity. It is generally known as a “Stealth Rule.” Rule 2 permits anyone on the Local Network to access any external network resource using the Telnet protocol. Rule 3 is designed to allow for web access during the Lunch hour only. Rule 4 permits only those clients who can successfully authenticate (User Auth) to access the internal web server using the HTTP protocol.

### Measuring Compliance

It is simply not enough to create policies, even good ones. It is not even enough to express these policies well. It is also necessary to measure the conformance to policies. The measurement of conformance is not simply an Orwellian task of micromanaging each and every keystroke of the employees at the business. The measurement of compliance has enormous value for the business.

Rule 5 is an important component of the rulebase for measurement. It is known as the “Clean Up” rule. If none of the other rules provides an exact match, this rule is finally executed by the firewall (Checkpoint, January 2000, page 278). At the policy level, this rule on the firewall drops packets which are not explicitly permitted by previous rules. In order to view these drops in the log file, the Track setting is set to “Long.” This setting gives us some very detailed information about each individually dropped packet such as the protocol, or network service being attempted, and the source of the attempt along with the destination.

No.	Date	Time	Inter.	Type	Action	Service	Source	Destination	Proto.
158	7Mar2002	23:56:45	 hme1	 log	 drop	domain	192.168.0.1	207.243.40.41	tcp
162	7Mar2002	23:56:46	 hme1	 log	 drop	1110	192.168.0.2	12.65.145.24	udp

### *Verifying business oriented behavior*

The measurements of not-accepted, or dropped, packets on the internal ports of the firewall represent network traffic which does not conform to the rules of the policy. This activity is by definition counter to the essential functions of the business.

In the above set of rules, which are an expression of the meta-rules, an allowance is made to permit users on the Local-Network to surf the web (HTTP) during Lunch (defined as from 12:00pm – 1:00pm). If a user tries to surf the web at 1:01pm, that packet will be dropped. Non-productive behavior, that is, behavior which ultimately does not add to the owner's long-term value can be identified by tracking these dropped packets

#### *Validating a new behavior requirement*

Beyond this, however, tracking of non-accepted packets can also reveal a heretofore unrecognized need. As an example, users on the Local-Network are permitted to use TELNET to any servers through the firewall. If there is an unspoken need for access to FTP services, these will show up as dropped packets. In this case, the dropped packets constitute an unexpressed or at least unspoken requirement to reevaluate the expression of the Meta-Rules. If FTP services are not counter to the Meta-Rules, then it would be reasonable to add an additional rule permitting FTP.

The measurement of compliance can be summarized as follows:

If an action does not conform to this policy, then one of two actions must take place:

1. Either the actions should cease or
2. The policy should be reviewed.

#### *Using Risk Measures as a Change Initiator*

*You can't run a business without taking risks. Pablo Picasso.*

The task of defining exactly how much risk a business can sustain before the situation becomes untenable is a difficult decision. There are no hard and fast rules. Anyone with a personal computer and the ability to click the NEXT button thinks they have solved the problem of risk by installing a personal firewall. But how does one really quantify risk in terms that will cause reevaluation of the expression of meta-rules and perhaps the meta-rules themselves?

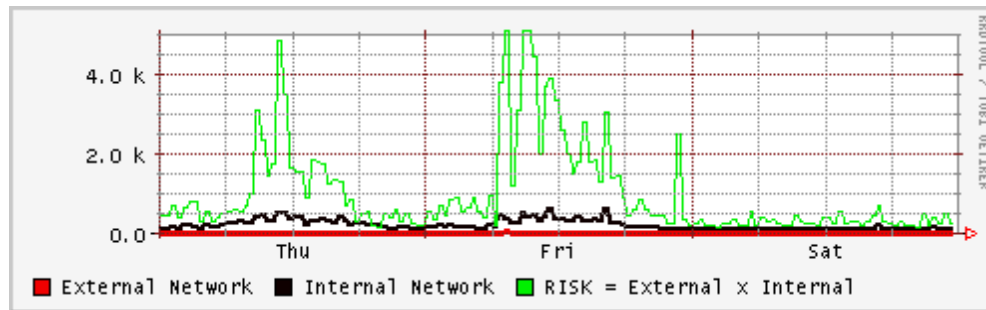
RISK is defined in a semi-mathematical way as

$$THREAT \times UNCERTAINTY = RISK$$

This shows that both THREAT and UNCERTAINTY have a special relationship to RISK. In an ideal world, these factors would be at zero, that is, there is neither a threat from external sources (that is, no one is trying to break in) nor is there any uncertainty (that is, all employees are operating within the confines of policy and the proper configuration of systems internal to your network). The goal of a good security policy should be to reduce risk by reducing threat, reducing uncertainty or reducing both.

Enforcing a good security policy on the inside port of the firewalls reduces, but perhaps does not eliminate, the uncertainty of non-core business activity. The measurement of compliance, that is, the inverse of drops and rejects on outbound packets, can provide a

metric for reducing risk by lowering uncertainty. On the outside of the firewall, the measure of the number of drops and rejects, provides a metric for estimating threat, or attempts to access internal system not permitted by the rules.



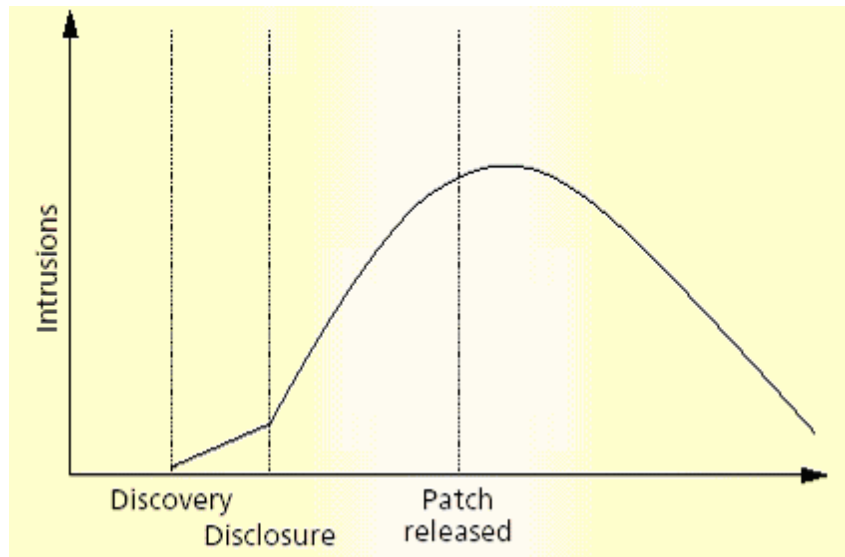
Taken together and over time, these two terms, can provide a baseline measure which shows a relative risk measure. If the baseline measure increases over time, changes to the expression of policy might be required. Additional security measures, such as ingress filtering at a border router or changing internal system configurations may also be required.

#### *Being Systematic about Measurements*

The first set of meta-rules, if carefully crafted and designed, will probably cover a large portion of the necessary policies and permit the creation of rules to meet the business objectives well. However, in the rapidly changing world of technology and commerce, it is clear that meta-rules cannot be defined in one sitting to cover every eventuality and needs for every locality and every division in an organization (Farnsworth, 2000). It is important to take a systematic and evolutionary approach to implementing security using meta-rules. (Hernandez, 2000)

Security is usually thought of in terms of events. The pace of life in security is often measured by events such as the release of a new worm or the discovery of a new exploit. This is not an unusual situation. As basic a science as paleontology argues that evolution (Gould, 1983) occurs, not in a series of small changes, but in an episodic, even jerky, method with large changes coming all at once, in a mechanism called punctuated equilibrium. But taken over time, these changes occur as an apparently organized assault on a single goal, the production of a new species. The discussion of vulnerability, too a sort of punctuated equilibrium has been proposed by Bruce Schneier. His (Schneier, 2001), and others' (Arbaugh et al, 2000) investigation divide the life-cycle of a software vulnerability into multiple stages. They theorize that the peak comes just after it is popularized in the media and hackers have encapsulated their knowledge in scripts which anyone (sometimes known as "script kiddies") can execute. The lifecycle of a single theoretical vulnerability is shown below as described by William Arbaugh and colleagues in December, 2000. Mr. Schneier includes a label on the rising curve from "Disclosure" to "Patch Released" as "Vulnerability Popularized."





In being so tied to responding to events themselves, there is rarely time for the security administrators to reflect carefully on the meaning of the events. Worse, there is the tendency to define security problems as something that can be solved by rules, regulation and enforcement. This is much like the discussion of preadolescent suicide by Daniel Quinn (Quinn, 1998), in which a governmental body is so intent on securing and removing the means of suicide that it fails to recognize that it is contributing to the problem. There might be a simpler method to stem the tide of suicides: find out why the preadolescents want to die and removing the motive! As is pointed out, the governmental body is in the habit of defining all problems as problems it can solve by doing what it was designed to do, make rules and enforce them. In other words, *“To the man who only has a hammer, everything begins to look like a nail”* (Jane Fonda).

But it is important to consider that the effectiveness of security can not really be evaluated by its response to a single event. Larry Miller (2001) of Mottahedeh Development Services wrote, “It [a systematic approach] includes identifying steps in a dynamic process, over time, and some way of reviewing the progress of those steps.” (Miller, 2001) Being systematic means to understand and work with this dynamic process of gradual improvement.

The security scheme must be capable of responding, not only to the threats from the external network, but also capable of responding to the needs of those on the inside network. Without the intention of careful, consistent and thoughtful review, the greater risk is that the security will no longer support the essential business objectives. When this is the case, the casual response is to eliminate the business roadblock, security.

To avoid this situation, establishing a learning mode is essential. Just as much emphasis must be placed on learning about the threats from the outside as is placed on understanding the needs on the inside. Measurements should be directed toward this goal and designed to learn about the system in which they operate. Thinking of security as a component of the business system where measurements help to visualize requirements

rather than a mechanism to control and punish refocuses measurements on a goal which increases its value to the business.

## **Discussion**

*“I can’t do my job” Every user I’ve ever known*

Why bother with all this?

“I can’t do my job” should not be viewed as a challenge to the security authority. Its underlying meaning is that the user does not know how to accomplish his/her objectives within the existing expression of the policy. The job of security is to use this as valuable information to review the security policy to make sure that first, this requirement doesn’t violate the meta-rules and second, and perhaps most important, that the requirement indicates a change has occurred within the business which justifies modification of the meta-rules themselves. With meta-rules, there is a common basis on which to rationally discuss the needs of the business. Without meta-rules, the discussion degenerates into who wields the most power or who can negotiate better.

The users of computers and networks are not security experts, and perhaps not even computer experts; their job is to do something ELSE within the business to increase owner long-term value. This “something else” and the objectives on which the security meta-rules are based must be consonant one with another. The meta-rules help users and even business owners understand what interests they have in common with security.

Most users and most business owners believe that security is an optional bolt-on function and not a piece of the core business. (Hart, 2001) For this reason, security is often seen as a business inhibitor, not a business enabler. It is important, especially in discussions with well-meaning users, to be able to show that the chain of rules, meta-rules and objectives lead clearly back to the purpose for the business. Meta-rules help form an understandable connection between the security rules and the business needs.

Policy is not simply a hammer used to hit a user over the head, in spite of how much his head looks like a nail. Policy is something that must be systematically reviewed to make sure it still meets the needs of the business and the needs of the people that comprise that business. Meta-rules have to be reviewed in terms of the objectives they are designed to accomplish. If the meta-rules don’t meet the criteria defined in the objectives, then the meta-rules themselves must change. Beware of the situation where risk is allowed to increase beyond the level of toleration simply to make the bottom line work. If risk is too high, meeting the bottom line may not matter – there will be no business. Meta-rules help form this risk boundary.

## **Future Inquiry Paths**

The concept of establishing meta-rules is not limited to the definition of firewall rules. Moving from basic, broad and underlying business objectives to more focused and specific rules is one that can be applied over and over to various areas of security implementation. Using this as a methodology, a clear and concise relationship between the business and its security can be carefully constructed.

Additional areas where meta-rules might help define a need are both ingress and egress filtering at the external or boundary router. Is the business, based on its economic function, responsible for egress filtering? How do meta-rules affect the creation of ingress filtering rules at the border between a business and the Internet and one business unit and other business units?

Are different meta-rules required for different divisions of the same business, or do can meta-rules be used in a hierarchical fashion?

Can meta-rules be used as a basis for change management of internal computer systems and network infrastructure to further minimize the uncertainty of introducing vulnerabilities?

Finally, could a better understanding of how the business objectives can be met with a defense in depth strategy can be encapsulated in the meta-rules?

© SANS Institute 2000 - 2005, AU

## References

All quotes used are available from URL: <http://www.brainyquote.com> (Mar 2002)

Arbaugh, William A., Fithen, William L. and McHugh, John, Window of Vulnerability: A Case Study Analysis, December 2000, URL: [http://www.cs.umd.edu/~waa/pubs/Windows\\_of\\_Vulnerability.pdf](http://www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf) (Mar 2002)

Brunton, Dick, Passion and the Purpose of Business, University of Auckland Business Review, Volume 3, Number 1 2001 URL: <http://www.uabr.auckland.ac.nz/articles/Vol3Issue1/vol3no1Passionandpurpose.pdf> (Mar 2002)

Checkpoint, VPN-1/Firewall-1 Administration Guide, January 2000, page 272

Farnsworth, William, What do I put in a Security Policy?, August 2000, URL: <http://rr.sans.org/policy/policy.php> (Mar 2002)

Gould, Stephen J., Hen's Teeth and Horses Toes, 1983, W W Norton & Company, New York and London

Hart, Badley, 2001, Implementing a Successful Security Assessment Process, URL: [http://rr.sans.org/securitybasics/sec\\_assess.php](http://rr.sans.org/securitybasics/sec_assess.php) (Mar 2002)

Hernandez, Ernest D., Network Security Policy – A manager's Perspective, November 2000, URL: [http://rr.sans.org/policy/netsec\\_policy.php](http://rr.sans.org/policy/netsec_policy.php) (Mar 2002)

Koretz, Gene, BusinessWeek Online, August 13, 2001, URL: [http://www.businessweek.com/magazine/content/01\\_33/c3745042.htm](http://www.businessweek.com/magazine/content/01_33/c3745042.htm) (Mar 2002)

Miller, Lawrence M., "On Becoming Systematic", Mottahedeh Development Services, URL: <http://www.mdssed.org/Education/TrainingTools.html> (Mar 2002)

New Riverside Dictionary, Riverside Publishing Company, 1988, Houghton Mifflin Company

Quinn, Daniel, Protecting the Environment: Whose Business is it? 1998, URL: [http://www.ishmael.com/Education/Writings/rice\\_u\\_2\\_98.shtml](http://www.ishmael.com/Education/Writings/rice_u_2_98.shtml) (Mar 2002)

Richards, Graham, Oxford University, 2002, URL: [http://search1.npr.org/opt/collections/torched/atc/data\\_atc/seg\\_138506.htm](http://search1.npr.org/opt/collections/torched/atc/data_atc/seg_138506.htm) (Mar 2002)

Riordan SJ, Patrick, The Purpose of Business and the Human Good, 1997, University of Saint Thomas, URL: <http://www.stthomas.edu/cathstudies/cstm/antwerp/p6.htm> (Mar 2002)

Schneier, Bruce, Closing the Window of Exposure: reflections on the future of security, Computer Security Alert, No. 215 February 2001 URL: <http://www.gocsi.com/pdfs/alert0201.pdf> (Mar 2002)

Schreiner, Mark, Meta-Rules, Microfinance Risk Management and Center for Social Development, June 2001, URL: <http://www.microfinance.com/English/Papers/Meta-rules.pdf> (Mar 2002)

Shaffer, Richard, Sun Was Right: Why the Network Is What Matters, Business 2.0, June 2000, URL: <http://www.business2.com/articles/mag/print/0,1643,7854,FF.html> (Mar 2002)

Sternberg, Elaine, Corporate Governance - Accountability in the Marketplace, Hobart Paper 137, Institute of Economic Affairs, 1998 (quoted by Patrick Riordan SJ)

© SANS Institute 2000 - 2005, Author retains full rights.