INFORMATION SECURITY MANAGEMENT

Information security assurance is a continuous crisis in the digital world. The attackers are winning and efforts to create and maintain a secure environment are proving not very effective. Information security assurance is challenged by the application of information security management. From one point of view, information security management evolved on using various security technologies promoted by the security industry and application of standards published by NIST, IETF, ISO/IEC, and other organizations. Quite often, these guidelines conflict with each other or they target only a specific type of organizations (e.g. NIST standards are better suited to government organizations). Therefore, information security management should be based on a framework that evolves to specific implementations.

A framework is the outline of the more thorough blueprint. The framework is the result of the design and validation of a working security plan which is then implemented and maintained using a management model. The framework serves as the basis for the design, selection, and implementation of all subsequent security controls, including information security policies, security education and training programs, and technological controls. The most popular security management model is based on the British Standard 7999 which provides components, each addressing a different area of security management practice.

The recent standards, called ISO/IEC 27000 family, include standards which replace BS 7799 standard. Similar security models are based on standards provided by organizations such as NIST Computer Security Center, IETF with The Site Security Handbook, and VISA with Cardholder Information Security Program.

However, building a security control framework focused only on compliance to standards does not allow an organization "to achieve the appropriate security controls to manage risk". Organizations need a systematic approach for information security management that addresses security consistently at every level. They need systems that support optimal allocation of limited security resources on the basis of predicted risk rather than perceived vulnerabilities. Security cannot be viewed in isolation from the larger organizational context and only based on technology. Security should be also based on non technical aspects. Besides technical security controls (firewalls, passwords, intrusion detection, disaster recovery plans, etc.), security of an organization includes other issues that are typically process and people issues such as policies, training, habits, awareness, procedures, and a variety of other less technical and non-technical issues. Security education and awareness has been lagging behind the rapid and widespread use of the new digital infrastructure. All these factors make security a process which is based on interdisciplinary techniques.

Information security management is broad and requires an intelligent approach because security is a complex system and must be considered at all points and for each user. Information security management has evolved lately from patching software and mitigating the exploitation of vulnerabilities to log analysis approach. The design of enterprise security perimeter is no longer a solid approach. Managing the security of any organizations require the applications of new paradigms based on process control methods as well as autonomic computing, autonomic networking, and machine learning approach.

GLOBAL CHALLENGES AND STANDARDIZATION

The nature of the organization and scope of information processing has evolved and managing information security is not just restricting to maintain information security services such as confidentiality, integrity, availability, and no repudiation. In the new millennium, there are demands for more responsibility, integrity of people, trustworthiness, and ethicality. Due to advances in communication technologies and reliance on electronic processing of data, organizations are challenged with maintaining good management practices, development of adequate policies to prevent and to deal with security problems.

INFORMATION SECURITY MANAGEMENT INFRASTRUCTURE

Information security management is the framework for ensuring the effectiveness of information security controls over information resources. It addresses monitoring and control of security issues related to security policy compliance, technologies, and actions based on decisions made by a human. Information security management objective is to ensure no repudiation, authenticity, confidentiality, integrity, and availability of the information within an organization. Although different security technologies support specific security functions, there are many issues that impact the efficient management of information security. A large percentage of the security software industry is built on the practice of looking for the digital patterns (signatures) that identify known threats. Anti-virus software based on pattern recognition accounts for more than half of the total security software industry. Also, firewalls employ the same technique of signature scanning that is flawed. Many spam filters classify email using “black” and “white” lists of the senders or relay servers. Some tools help email system managers update black lists, but the overhead remains burdensome because spammers can easily spoof email senders or relay servers using end-user machines.

The information security management is based on its own infrastructure on top of a network management infrastructure or integrated with the network management infrastructure. Therefore the evolution of information security management is mostly affected by the current security technologies that lack integration and rely on human for analysis of huge data collected. However, the information security management infrastructure will be mostly affected by the most recent paradigms of autonomic computing and later, autonomic networking that address the operational complexity of communications networks.

EFFICIENT AND EFFECTIVE SECURITY MANAGEMENT SOLUTIONS

Although network management has always played a key role for the communication networks, it only recently received a similar level of attention from many research communities, accelerated by funding opportunities from new initiatives, including FP7 Program in Europe and GENI/FIND in the United States. Research directions to be pursued over the next five years include management architectures, distributed real-time monitoring, data analysis and visualization, network security, ontologies, economic aspects of management, uncertainty and probabilistic approaches, as well as understanding the behavior of managed systems.. These

developments may trigger impetuous advances in the quality of the security products including efficiency and effectiveness of information security management.
New developments as well as sales of the security products are estimated to grow worldwide. Gartner estimates that security software revenue will increase at a rate of 10.4% from nearly $8.3 billion in 2006 to more than $13.5 billion in 2011.

The many aspects of managing information security can also be classified as being strategically, tactically, or operationally oriented. Strategic information security management addresses the role of information resources and information security assurance infrastructure over the long term. It is focused on ensuring the organization has the information security infrastructure that it needs to achieve its long-range business goals and objectives. An important aspect of strategic information security management is the creation of security plans that specify how the organization's security infrastructure (including its communication services, networks, and interfaces with customers and business partners) will change in the near future and long term. It should address how new and emerging communication technologies and applications (such as wireless applications) will be incorporated into the information security management infrastructure. Data management, risk management, and contingency planning are other strategically oriented activities. Essential to any business are new strategies such as

- Protecting intellectual property
- Use of security metrics that are shared across organization to help in better decision making
- Investing in security from reactive add-ons to proactive initiatives that are aligned with the company's strategic goals
- Building a secure culture based on education and ongoing discussions.

Tactical information security management includes the translation of strategic security plans into more detailed actions. Tactical information security management involves the development of implementation plans and schedules for implementing new security technologies. Other important tactical management functions include selecting vendors, training users and administrators, and developing follow-up evaluation and maintenance plans.

Operational information security management concerns the activities associated with managing day-to-day security operations of an organization. Best business practices models including log analysis do not always provide the greatest level of performance in the protection of the information. Thus, a small shift in perception (from viewing data as a cost to regarding it as an asset) can dramatically change how an organization manages the data.

To deliver protection against the latest generation of cyber threats, the rules of preemptive protection have to meet criteria for effectiveness, performance, and protection. Effectiveness of security management system is determined by the intelligence of the system, defined as the ability to detect unknown attacks with accuracy, along with enough time to strategically take action against intruders. Efficient information security management requires an intelligent system that supports security event management approach with enhanced real-time capabilities, adaptation, and generalization to predict possible attacks and to support human's actions. To provide a complete, accurate, and comprehensive picture of network events that is desired by

network administrators, a huge amount of event processing in near real-time, consolidation, and correlation of events are required. There is also a growing need to extract and highlight the unusual traffic and unusual traffic patterns, real-time analysis and visualization, to reduce detection and reaction time. Especially for security auditing purposes, it is often much more desirable to find and locate small volume but highly unusual traffic streams or patterns.

Management is fundamentally about deciding and delivering behavior. Researchers want to model and manage the behaviors of hardware, software, and even users with a system. Behavior implies the ability to predict changes in a system, either changes made autonomously or in response to input (events or programming). However, behavior can be understood empirically or theoretically.

The existing challenges of information security management combined with the lack of scientific understanding of organizations' behaviors call for better computational systems that support effectiveness of using specific information technologies and new approaches based on intelligent techniques and security informatics as means for coordination and information sharing. Information security management requires supporting functions such as the following:

Management of heterogeneous devices and security technologies
Since different security technologies provide different management data, describing the same or similar concepts, it is imperative to harness information models and ontologies to abstract away vendor-specific functionality to facilitate a standard way of aggregating and viewing the data. Achieving this will enable all information security tools and information resources with no inherent autonomic capabilities to be managed ay autonomic systems.

Adaptability
One of the promises of autonomic operation is the capability to adapt the functionality of the system in response to changes in policies, requirements, business rules, and/or environmental conditions. In particular, the information security management system must sense context changes and use policies specific to the new context to effect the required actions.

Learning and reasoning capabilities to support intelligent decisions
Statistics can be gathered and analyzed to determine if a given device is experiencing a cyber attack. This information must be inferred using a security knowledge base and other data and retained for future reference. There is a need to incorporate sophisticated, state-of-the-art learning and reasoning algorithms into information security management system.

Control model
Using closed and open loop process control approaches, we can more accurately set an acceptable limit of risk, build trust, and thus protect the organization more effectively.

Decision making
Using monitoring data, we can automate decision making and taking actions to control the behavior of the device, applications, or system thus preventing cyber attacks.

Intelligent assistant

Security personnel can use an intelligent approach to identify key areas where the system requires human intervention or the human requires advice on making decisions. Human intervention will be required for the refinement of policies and also to resolve policy conflicts never before encountered by the system.

Building knowledge

The vision of intelligent systems for information security management is that of a self-managing security infrastructure that itself can access, or generate, the knowledge it requires to enable it to optimally react to changing of policies or operational contexts.

CONCLUSION

Information security management includes aspects of strategical, tactical, and operational activities. Transferring cyber security risks to another party may open a new spectrum of issues.