

Principles of Survivability and Information Assurance

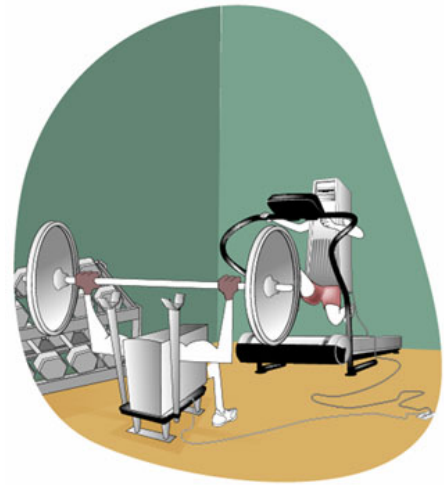
*Lawrence R. Rogers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213*

Organizations and individuals alike want their technology to survive attacks, failures, and accidents, but the technology in computer systems, software, and network infrastructure components changes frequently and is vulnerable to disruption. System administrators, a term which can now apply not only to professionals but also to owners of home computer systems, need a solid educational foundation in order to react to technology changes, minimize disruptions, and manage their computer systems and network infrastructure components. The ten principles of survivability and information assurance described here create just such a foundation.

Principle 1: Survivability is an enterprise-wide concern.

Survivability, in the context of computer security, is the capability of a system to fulfill its mission in a timely manner, despite attacks, failures, or accidents. As a concept and as a practice, survivability should permeate all levels of an organization. Staff roles contribute differently to the overall goal of organizational survivability, from leadership, which makes decisions setting security policy, to system administrators, who recommend and install technology in support of survivability. An organization-wide understanding of the importance of survivability contributes to long-term growth and mission fulfillment.

References: Paper: "Survivability - A New Technical and Business Perspective on Security". Proceedings of the 1999 New Security Paradigms Workshop. Caledon Hill, ON, September 21-24, 1999. New York, NY: Association for Computer Machinery, 2000 (<http://www.cert.org/archive/pdf/busperspec.pdf>).



Principle 2: Everything is data.

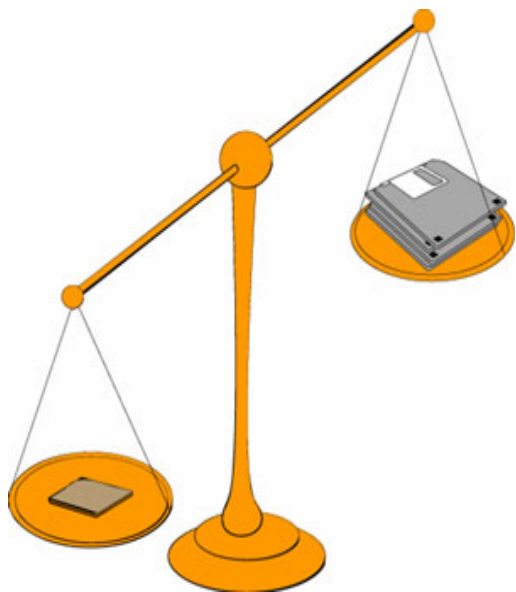
Everything in and around a computer system, network infrastructure component, and survivable functional unit¹ can be understood as data. This perspective is useful because it helps staff define and manage information that needs to be protected and then to decide how to protect it. Understanding that an organization's data exists throughout various states such as storage, transmission, and processing, helps system administrators (SA) understand the need to use tools and techniques such as network sniffers, access control lists, encryption, and strong integrity.

¹ A survivable functional unit (SFU) is a collection of computer system and network infrastructure components that delivers information assets through one or more services to various constituencies that are authenticated to the survivable functional unit. The SFU provides essential services in the presence of attacks and failures, and recover full services in a timely manner.

In information security, there are three attributes of data (often referred to as the InfoSec triad) that should be considered and secured: confidentiality, integrity, and availability (CIA). The places where data reside and the general techniques that should be used to protect their CIA attributes are all defined in a government publication NSTISSI 4011: National Training Standard for Information Systems Security Professionals (<http://www.nstissc.gov/Assets/pdf/4011.pdf>).

References: *File Cabinets and Pig Latin: Guards for Information Assets* (<http://www.cert.org/homeusers/piglatin.html>).

Principle 3: Not all data is of equal value to the enterprise – risk must be managed.



Every organization has a variety of information assets. These information assets – often referred to as data – are not all of equal value. By understanding the relative importance of each information asset to the organization’s mission, system administrators can direct the survivability efforts towards protecting assets based on their criticality and priority.

There are various methods to conduct an information security risk evaluation to identify an organization’s most important information assets. One of these is OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM), a risk-based strategic assessment and planning technique for security (<http://www.cert.org/octave/>).

System administrators need to know about risk management because they cannot protect all assets. Security procedures and technologies are risk mitigation techniques that need to be selected and managed to minimize risks to critical information assets.

Principle 4: Information assurance policy governs actions.

Information assurance can be understood as the information operations (IO) that protect and defend information and information systems (IS) by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

System administrator activities should be governed by organizational and security policies which define acceptable and unacceptable behavior for all users.

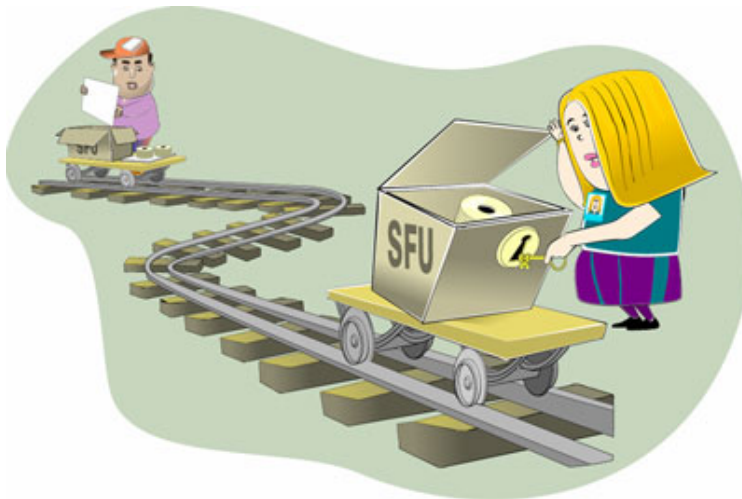
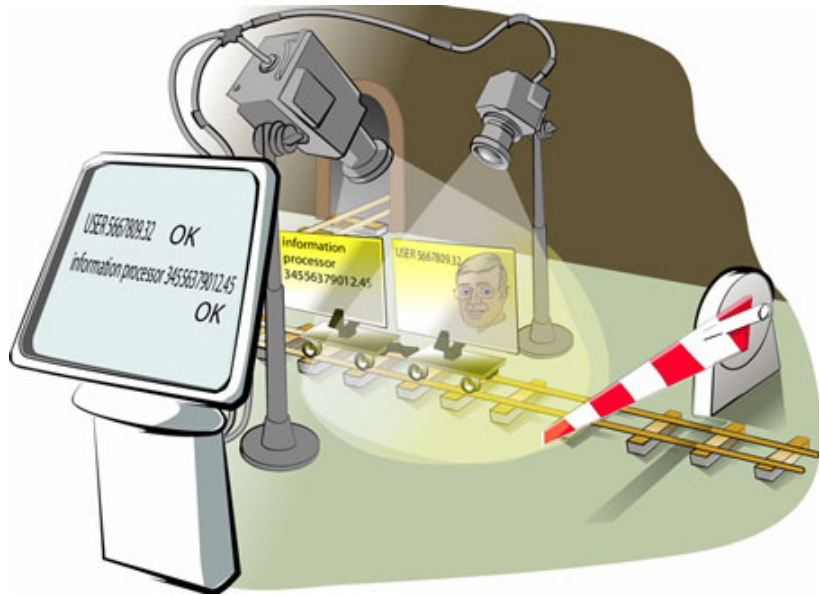
Administrators need to understand the importance of documenting, implementing, and enforcing policies that are regularly reviewed, updated, and reflect their role.



Principle 5: Identification of users, computer systems, and network infrastructure components is critical.

System administrators create secure access to an organization's information assets based upon user identification. No matter how strong the information access technology, if it is based on weak user identification, it is effectively irrelevant. System administrators need to know that reliable, strong, and useable user identification is the foundation upon which restricting access to information assets is based. To achieve these goals, they need appropriate technology and a policy that complements it.

System administrators also need to identify infoproc² in a reliable, strong, and usable manner. For example, they should know with certainty that the computer system to which they are making a network connection is the one they believe it to be. Also, they must know that the infoproc attached to their network infrastructure are the only ones so attached, and that they have not been impersonated.



Principle 6: Survivable Functional Units (SFU) are a helpful way to think about an enterprise's networks.

Survivable functional units are a collection of computer system and network infrastructure components that deliver information assets through one or more services to various constituencies that are authenticated to the survivable functional unit. The SFU should be constructed to provide essential services in the presence of attacks and failures, and recover full services in a timely manner.

Infoproc – the sum of users, computer systems, and network infrastructure in the organization – are part of SFUs and each one should possess a descriptive architecture accompanied by a set of questions the system administrator should consider when sustaining and improving existing functional units and building new ones.

References: *Survivable Functional Units: Balancing an Enterprise's Mission and Technology* (<http://www.cert.org/archive/pdf/04tn004.pdf>).

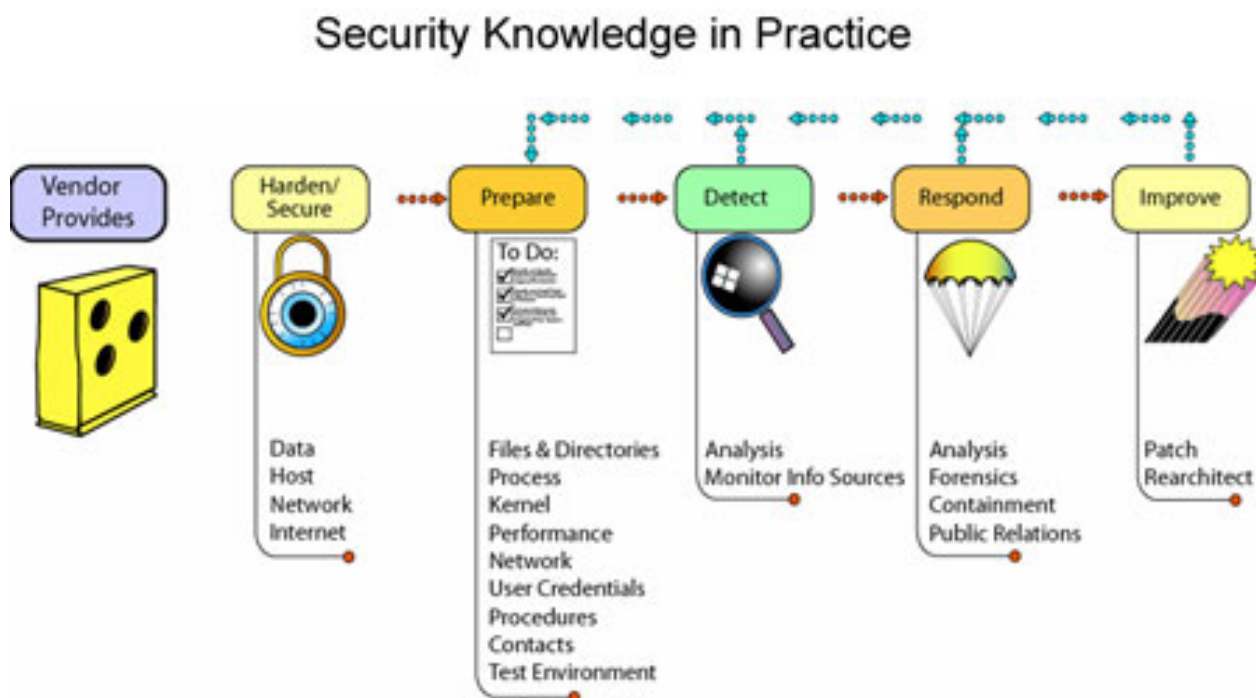
² Infoproc is a term used to refer to the sum of users, computer systems, and network infrastructure of an organization.

Principle 7: Security Knowledge in Practice (SKiP) provides a structured approach.

A system administrator needs a structured approach to sustain and improve the survivability of SFUs and their constituent computer systems and network infrastructure components. The Security Knowledge in Practice (SKiP) (<http://www.cert.org/archive/pdf/SKiP.pdf>) method is such an approach. It is an iterative improvement method that structures and orders the CERT Security Improvement Practices. These practices are designed to improve the security of computer systems and networks during their complete lifecycle.

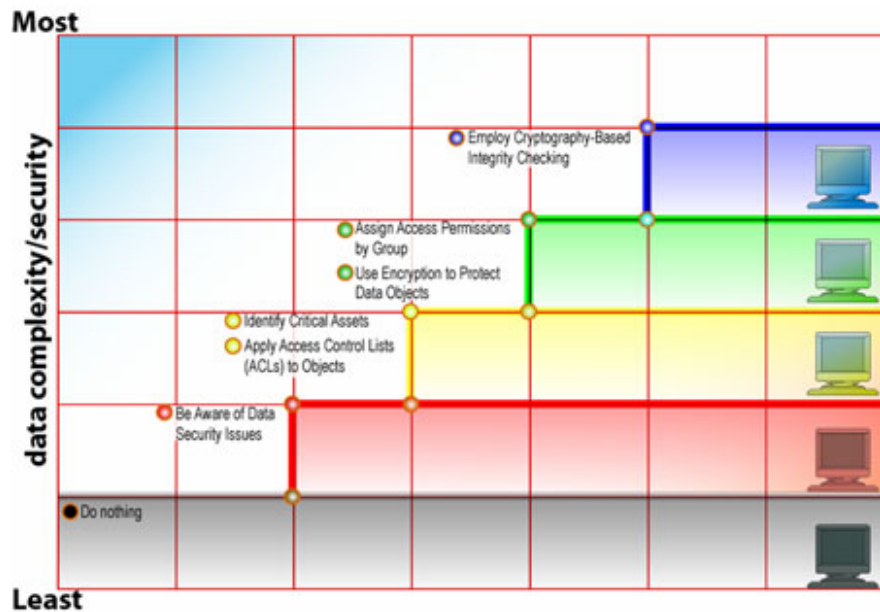
SKiP can be applied at the host level, the network architecture level, and at the SFU level. In practice, it should be applied at all levels. SKiP is the foundation for performing survivable systems administration. It helps the system administrator know what they are doing to an SFU, a computer system, and the network. Administrators can identify what steps in the process they have executed, where they are currently, and what to expect as their next set of actions. SKiP is best applied after conducting a risk evaluation of an organization's information assets.

References: *Securing Information Assets: Security Knowledge in Practice* (<http://www.stsc.hill.af.mil/crosstalk/2002/11/rogers.html>)



Principle 8: The road map guides implementation choices (all technology is not equal).

It can be an overwhelming task to wade through the wide range of public domain, commercial, and custom security products and tools. The technology roadmap shows various levels of sophistication and complexity in the choices of technology available to system administrators. It gives system administrators introductory concepts and a structure they can use to make reasoned choices about which security technologies to select and deploy to enhance survivability.



The technology roadmap incorporates the concept of progression and sequence, building from awareness to adequate protection to more sophisticated solutions.

Red means danger, ignorance, and negligence if the organization is unaware of the important considerations in protecting each asset category. Yellow connotes actions that an organization should take as soon as possible. Green indicates an acceptable level of protection compared to standard deployment choices of many other security-conscious organizations. Blue is more advanced and should be driven by business needs, policy, security requirements, and asset criticality.

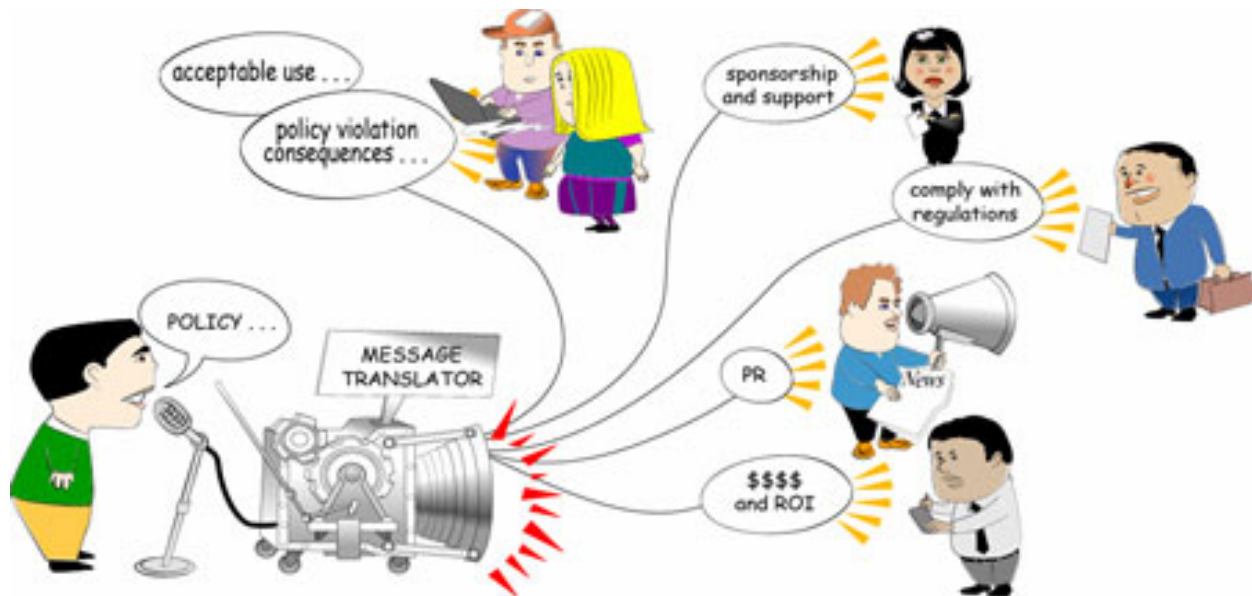
Principle 9: Challenge assumptions to understand risk.



System administrators need to learn to “think like an intruder” including assessing the vulnerabilities of the technologies in use at their organization. By regularly scanning for weaknesses and vulnerabilities in deployed technology, system administrators learn to enhance survivability and improve security. By not blindly accepting a default implementation of a given technology, a system administrator can gain valuable experience that allows them to document their assumptions, which is a core part of their professional responsibilities.

Principle 10: Communication skill is critical to reach all constituencies.

System administrators need to be able to adjust their language based on their listener. For example, when communicating with upper management, the language should be less technical and more business-oriented than when talking to a fellow system administrator. To be effective, technical messages must be conveyed in a style that can be clearly understood and evaluated. To gain a manager's trust, confidence, and understanding, the system administrator needs to demonstrate that they care about the business as much as they want the manager to care about security.



The system administrator must also learn some of the ways of business and be prepared to translate business terms into the appropriate actions at a technical level. Understanding risk evaluation methods such as OCTAVE helps them to be better equipped to deal with the realities of business and do their part to support the organizational mission.

All employees in an organization should recognize that information survivability is a fundamental principal and that achieving and sustaining survivability requires a collaborative effort. This means that the system administrator must be prepared to talk with many people in the organization to achieve information survivability. Communication skills are a key element.

Summary

Technology and the training that builds skills that support technology are equally volatile. Education bridges the gaps in knowledge created by the inevitable changes in technology. A thorough understanding of the principles of survivability and information assurance creates a firm educational foundation designed to address the knowledge gaps that arise in the area of information technology security.