



Control Essentials

Defense In Depth



Information security is best evaluated by examining the return on investment. And not necessarily just the ROI by your organization; but by the ROI of the effort by potential attackers. How difficult do you make it for them?

Any organization trying to protect itself from threats to its information assets should logically try to ensure that an attacker's overall effort, cost, and risk involved is very high. An attacker, on the other hand, would try to minimize this cost and maximize the return.

Savvy organizations will always try to minimize ROI for potential attackers. How to do it involves a technique that has been around a long time.

Defense In Depth

Defense in depth was originally a military maxim that was adapted into the information security world. The military strategy aims at delaying an attacker's advance. By doing so, the consequence of the attack is not only weakened in impact but also buys the defender time to deal with the attack effectively. The technique ensures that the time delay also leads to a loss in momentum and focus of the attack.

This military technique has found its way into the information security arena with measurable success. The focus in information security, though, is to have multiple layers of protection in place to ensure that even if one of the layers on the outside fails there is an inner layer to fall back on, which can further fall back on more inner layers.

The method is not new at all. It is a principle that you would have most likely used in your day-to-day life at some point of time. For instance, a personal safe in your bedroom has a secure lock. You might lock your bedroom for added safety when you're going out of the house. And, finally, you'd lock the house itself. These multiple layers of protection ensure that even if a thief was to pick or break the main house lock, he'd be faced with further layers of protection. These layers are, at times, enough to put off the thief who might think that the return on investment from his effort is not very high.

In ancient war times, cities were often built with multiple layers of walls so that if the outer walls were breached by an attacker, he would still face the prospect of repeating the feat over and over again with the inner walls. Such a design can be seen even today, for instance, in army establishments such as the Pentagon.



Defense in depth is like an onion. Each layer protects the inner one immediately following it until the core is reached which holds the valuable information asset.

The Evolution

Before the advent of defense in depth in information security, it was believed that perimeter hardening offered a sufficient amount of protection to organizational infrastructures. The method was successful only until it became clear that a single perimeter, albeit well-fortified, is also a single point of failure.

Defense in depth emerged as the evolutionary next step in IT security. It offers a bigger challenge to the implementers, but has emerged as one of the most effective and efficient methodologies to protection information assets today.

A Closer Look

To be able to use defense in depth at your organization, a better understanding of it is essential. Defense in depth involves three critical components:

- People
- Technology
- Operations

For an organization to be able to effectively implement defense in depth, it must understand and implement the right mix of these components. Let's take a closer look at each of these components and see exactly how an organization would implement a robust defense in depth framework.

People

The people of an organization are the implementers of information security. For this very reason, they also logically become its weakest link.

Roles and Responsibilities

The people of an organization must be well versed in their precise roles and responsibilities. These should further be directly derived from the policies, procedures and objectives of the organization. When roles and responsibilities are fully understood and diligently followed, the organizational policy gets implemented automatically. People in the organization will have a responsible attitude towards information security and a feeling of ownership towards the organization.

Managing attitudes is one aspect that often takes a backseat in the daily hustle-bustle. However, it is vital to ensure that employees receive a pat on the back for responsible attitudes and diligent abidance to their roles and responsibilities. At the same time, reprimanding those that exhibit non-compliance and difficult attitudes is equally important.



Awareness and Training

Security awareness training is very important to ensure that employees understand the implications of their actions on the overall security of the organization. Often, the people of an organization turn into the weakest link due to lack of basic awareness. With appropriate awareness training, employees become more observant and begin to appreciate the role of information security.

Social engineering engagements are very useful in exposing the weaknesses in an organization's human firewall. The findings of these engagements should be fed back into ongoing security awareness efforts. This way an organization can achieve a highly targeted and result-oriented awareness training program.

Providing skills training is as important as security awareness training for employees. Information technology changes by the minute. Employees that work with information security and information technology should receive regular training to enhance their skills and keep abreast of all the latest advancements. And when these employees return from training, they also gain new ideas and methods that can take the organization forward.

Physical Security and Personnel Controls

Even in the modern technology age, physical security and personnel controls play a key role in ensuring the security of an organization's infrastructure and information assets. Sometimes no amount of technical security can replace physical security to avoid information simply "walking off" the premises. Monitoring systems should ensure that physical access to the organization and, particularly, key areas of the information technology environment are kept under close surveillance at all times. Employees within the organization also need to be monitored to minimize the possibility of an insider threat materializing.

Technology

After people, technology forms the next line of defense in an organization.

Design and Implementation

An organization's network topology design and implementation should be audited periodically. Often, it turns out that the real reason for a security breach was not a problem in the implementation but the blueprint that was used in the implementation. A multi-layered topology can ensure that defense in depth is efficiently implemented so that if an attacker were to gain unauthorized access to an outer segment of the network the inner ones would still be safe. Network segmentation and network traffic control are two key aspects of secure design and implementation. Firewalls, routers, intrusion detection systems, and anti-viruses are great for security, but only if they are correctly placed.

Technical Audits and Assessments

Technical audits and assessments are not new at all. However, often organizations do not take advantage of the full array of audits and assessments available.



- A risk assessment plays an important role in any defense in depth implementation effort. Risk assessments provide an organization with the exact picture of what needs to be addressed, in what order of priority, and with what kind of resources. Once this is known, further technical audits and assessments can be performed in a targeted manner.
- Penetration testing should be conducted to examine both internal and external levels to ensure that the organization's network is fully secure. Such tests should also be performed at an application level where the organization's website and other applications, both internal and external, become part of the audit.
- Information security audits and comprehensive vulnerability assessments then take care of the nitty-gritty aspects like configurations and deployments.
- Analysis of security logs is also a very useful way of keeping track of what goes on in an organizations' technical infrastructure.

Incident Response

The true strength of an organization's information security capability is tested at the time of security incidents. An organization must have a premeditated incident response plan in place to ensure that security incidents are appropriately escalated and handled. The plan should have formal escalation levels, escalation triggers, specific actions, and key contact information. An incident response plan must also be tested and updated on a periodic basis to ensure that it is fully up-to-date and capable of dealing with incidents. An outdated plan might be helpless in the face of an incident that uses new techniques and attacks.

Operations

Last but not least, the operational layer of an organization forms a layer of defense that could prove to be the difference in the long-term security of organizational information assets and infrastructure.

Business Continuity

Organizations must have a comprehensive business continuity plan in place to ensure that operations can continue profitably and smoothly in the event of a contingency. Such situations could range from natural disasters and terrorist attacks to network and connectivity downtime. A business continuity plan becomes essential in modern times considering the amount of dependence organizations have on technology.

Business continuity plans must include detailed, step-by-step instructions in case of a contingency. Key departments of the organization and essential functions need to run smoothly, with the transition from normal operations to contingency operations occurring almost seamlessly. Testing and updating the business continuity plan on a periodic basis with documented test results and future improvement actions is vital.



Compliance

While compliance might be looked upon curiously in the defense in depth context, it is important to note that it is a business enabler. An organization needs to be in compliance with all applicable regulations if it is to conduct business smoothly.

Organizations must monitor all applicable regulations to ensure complete knowledge which can transform into compliance. New regulations must also be analyzed to ensure that if the organization newly becomes subject to compliance, it can take the necessary actions and measures to be compliant.

At all times, be aware and cautious of your budget. Compliance often derails organizational budget plans without prior warning.

Organizational Leadership

Information security doesn't happen by default. Organizational leadership needs to proactively and responsibly address information security needs periodically. A responsible attitude would demand that board meetings include information security on the discussion agenda. Key members from the information security and information technology departments should be included in such meetings to give and receive valuable input.

Overall, a responsible attitude at the top rungs of the organizational hierarchy will always trickle down to all employees. First-line employees are the first line of defense. Hence, good organizational leadership can strengthen the innermost as well as the outermost layers of defense at the same time.

The More The Merrier

Over the past decade, defense in depth has proven to be a highly effective and useful strategy for implementing robust organizational information security. Of all the facets of physical combat that found their way into their logical counterpart, defense in depth has surely been one of those that stand out.

Two shields are better than one. The more the merrier.

ERM wants to hear from YOU....

With this edition of our newsletter, we're rolling out a new format and new features. Tell us what you think!

What features or topics would you like to see covered in future issues? Who else should receive this newsletter?

Your feedback is welcome and encouraged. Please send your comments to editor@emrisk.com.

Enterprise Risk Management: *At a Glance*

ERM brings clients the highest level of expertise to assess and address risks, comply with standards and regulations and mitigate risks, using integrated and reasonably priced security services and solutions.

Our practice provides organizations with the tools they need to address the compliance and risk management issues of today, as well as the broader and ever-increasing security challenges of the future.

Services

IT Security
Regulatory Compliance
IT Audit
Computer Forensics
Risk Management
Attestation

Certifications

Certified Public Accountant (CPA)
Certified Information Systems Security
Professional (CISSP)
Certified Information Systems Auditor (CISA)
Certified Information Systems Manager (CISM)
Certified Information Technology
Professional (CITP)
GIAC Security Essentials Certification
GIAC Systems and Network Auditor
Qualified Security Assessor (QSA)
Approved Scanning Vendor (ASV)

Some of our Clients

ABN-AMRO Private Banking
Bacardi-Martini, Inc.
Bancafe International
Banco Industrial de Venezuela
Banco ITAU
Bank United
Caja Madrid Bank
Carnival Cruise Lines, LLC
CitiBank
Coconut Grove Bank
Commerce Bank
E-data Financial
Florida International University
Florida Power & Light Company
Heico Aerospace
Helm Bank
Knight Ridder
Nova Southeastern University
Rinker Materials
Rudy, Exelrod & Zieff, LLP
Seabourn Cruise Line
TecniCard, Inc.
The International Bank of Miami
TransAtlantic Bank
U.S. Century Bank

For more information, visit www.emrisk.com

E-mail: info@emrisk.com

Phone: 305-447-6750

800 Douglas Road
North Tower, Suite 835
Coral Gables, FL 33134

enterprise risk management

The Control Professionals