C)ISSO +
A Prep Guide to the CISSP® Exam

Based on the content of the C)ISSO, CISM®, and CISSP® Certification Examination Outlines

KEVIN HENRY C)ISSO, CPTE, CISSP-ISSMP, CISM, CRISC, GIAC

Mile2
11928 Sheldon Road
Tampa, Florida, USA
33626

First published in the United States of America in 2014
by Mile2 Publishing.

PREFACE

How to keep secrets and protect information is a challenge that has been around since the first time a person wanted to hide a piece of information from someone else. Maybe it was a good hunting or fishing spot or a secret to growing better food. Regardless, the possession and protection of this knowledge provided the holder of the information with a significant advantage over those that did not know the secret, or perhaps even assured survival itself.

Not much has changed - we still have information - and we still have secrets. We have seen, and continue to see that the loss of that information may lead to the loss of a battle, loss of competitive advantage, and even threaten the survival of a company, a nation, or an individual.

Protecting information is dangerous, especially in a world of access, technology, and networking. The threats are not just the company next door or anyone with physical access. The risks indeed are global, and a breach may happen from anywhere in the world People that we may never meet, have never even heard of, and are not bound by our laws, standards, and ethics.

The world of today needs experts that not only need to or want to protect information but also know how to do it. Enthusiasm is great, and having a passion for what we do is essential. However, that enthusiasm is not enough. Expertise, knowledge, wisdom, and the ability to perform the actions and responsibilities associated with the task at hand are also needed.

A master cabinetmaker can create a work of art, a desk or table which will last for hundreds of years. He can bring out the best qualities of the wood and through the skilled use of tools and procedures, transform materials into products that are fit for purpose, creative, and effective. But all tradesmen will tell you that the first secret to success starts with using the right tools. Balanced tools, forged from quality steel, and are designed for a defined purpose. (Even a good hammer cannot adequately replace a wrench). But each tool must be configured correctly - sharpened, clean, and maintained so that it will work when needed. So also is the first secret to information security. The security professional must start with tools that are designed for the purpose and properly maintained. One must keep the security rules sharp and accurate, doing regular review and maintenance of the tools, and skillfully using the tools available to achieve the desired result.

The second and third secrets are people and procedures - but we will get into those later in the book. This is a preface, a quick introduction to the value and content of this book. We will provide you with the information to master information security and management. And we are equipping you to do work that will stand the ravages of time, use, and an ever-changing world of threat and risk management.

ABOUT THE AUTHOR

Kevin Henry CISSP-ISSEP, Sec+, CBCI, CISM, CISA, CRISC, SCF

Kevin Henry is a well-known and respected educator and lecturer in the fields of Information Security and Secure Applications Development. Kevin uses over 30 years of practical experience as a network technician, computer programmer, and information systems auditor to deliver outstanding presentations. He makes each topic interesting, relevant, and useful. Students often describe him as ‘The best instructor I have ever had.’ Kevin can provide quality instruction that engages the audience and provides guidance on how to implement a successful program when they return to their workplace.

Kevin’s experience includes helping develop information security programs for numerous clients in North America, the Middle East, and Africa, and assisting in the development and delivery of courseware for many of the leading certification organizations in the world, including (ISC)2, ISACA, BCI, and Mile2.

Kevin has written several published papers and chapters for textbooks and study guides on the field of Information Security as well as being invited to speak at numerous conferences every year on these subjects.

ACKNOWLEDGMENTS

For many years, my wife and children had watched me leave for other countries, with the suitcase and laptop in hand. Weeks later, they welcomed me back with the same love and enthusiasm they had when I left. This book is dedicated to them, for no person can achieve their full potential without support and encouragement from their friends and family. Their undying strength that such people provide inspires and sustains me. To be married to your best friend and have the blessing of an incredible family is something no person can take for granted or ever deserve. I have received in life, more than I could ever have dreamed, much better than I deserved. For God's goodness and the goodness, kindness, and understanding of each of my family and friends, I am genuinely grateful.

CONTENTS

INTRODUCTION

What is security?

Security is the degree of resistance to or protection from harm. It applies to any vulnerable and valuable asset, such as a person, dwelling, community, nation, or organization. (en.wikipedia.org)

1. Freedom from danger, risk, etc.;
2. Freedom from care, anxiety, or doubt.
3. Something that protects or makes safe;
4. Freedom from financial concerns.
5. Precautions are taken to guard against crime, sabotage, etc.
6. A department or organization is responsible for protection or safety. (thefreedictionary.com)

The term security has many meanings and is applied differently in different contexts. This is often the first challenge for a security manager. The security manager is faced with defining and describing the security function and promoting the benefits and advantages of a security program. This is difficult when the very definition of the term is misunderstood and may even be incorrectly defined by the senior managers, users, and other stakeholders of the organization. Security is often associated with an emotional state or perception instead of hard evidence or measurable benefits.

On top of this, the security department often misunderstands its role in the organization. The purpose of security is not to "catch the bad guys" or enforce the rules. The use of protection is to support the aims and mission of the business and protect the organization from harm, loss, fear, and anxiety. Moreover, the real role of the security team is to serve the organization - to be an integral part of the business processes.

Information security is the protection of information - ensuring the defense, stability, and availability of the data and systems needed to support business objectives. As will be seen in the book, information security is a complicated and broad field and encompasses nearly every aspect of business today. The information must be protected throughout the information lifecycle - at all times, from the initial gathering of the information, through its processing, storage, transmission, and reporting, until the day it is discarded. Information on systems, networks, and paper. A breach is not just the theft of information by an outsider. It may also provide access by an unauthorized insider, the contamination or release of data intentionally or accidentally — the failure of equipment that was meant to protect the data and the circumvention of the business procedure. Just as information touches every area of business today, so also does the task of information security - reaching into the realms of physical security, law, business continuity, and compliance.

The information must be protected at all times, in all places and all forms. This is what makes the field of information security management exciting, ever-changing, and rewarding.

The layout of this book

One objective of this book is to help a candidate prepare for ISACA's Certified Information Security Manager (CISM®) certification or (ISC)2’s CISSP®... This book follows the structure of the current standards in Security Management including the ISO/IEC 27002 - Security Techniques - Code of Practice for Information Security Management, ISACA's COBIT version 5, the Sherwood Applied Business Security Architecture (SABSA), and (ISC)2's CISSP® CBK®, among others. This book is intended to assist a person wishing to advance their knowledge and an overall understanding of the fantastic field of information security management. Perhaps towards obtaining a certification such as Mile2's C)ISSO, ISACA's CISM®, SANS GSLC, or (ISC)2's CISSP®, but most of all the purpose of this book is to provide meaningful benefit to the person wanting to be better at their job responsibilities in the field of information security.

The examples used in this book are real and demonstrate the challenges faced by many security professionals. Hopefully, we can all learn from their experiences and benefit from the lessons they have learned. The book is intended to be practical, not just theoretical. Still, we have learned over the years that knowing some of the history and theory behind why we do certain things may also be invaluable in helping us understand how to leverage the lessons of the past and avoid repeating the same mistakes.

In summary, the most benefit from this book can be obtained by seeing the topics as:

- Practical, not just theoretical.
- Useful, not just conceptual.

This book is not intended to teach all the practical steps a security practitioner must follow or teach how to use various tools. This book is designed for the security professional, the manager, the person responsible for setting up, managing, operating, and reporting on security and taking a leadership role in protecting the organization. As you read this book, please pay attention to the concepts behind the examples, not just the cases themselves. Try to apply the concepts covered to your real-world situations; challenge your current beliefs, and consider all the angles and approaches used by other professionals in the field. As we should all know, there is no one perfect way to solve every security challenge and no way to ensure that the answers we used yesterday will be useful in the future.

The Relationship between Security, Engineering, and Architecture

The first area a security manager must understand is the relationship between Security, Engineering, and Architecture. Security management requires a combination of skills and an integrated approach to building a security system that can withstand the attacks it will face. This involves the use of technology, but technology itself is not enough. Technology must be used in the right way, by people that have been trained in its use, and supported by all the other elements of the complete security framework. Knowing the way to design (architecture), build (engineering), and maintain a security framework that balances security requirements with business objectives is the critical attribute of security management professionals.

The security professional must be able to quickly adapt to changing threats and be flexible enough to accommodate new technologies, business practices, and standards - in most cases, with insufficient funds, resources, or support!

Architecture is the planning, designing, and building of a security program that brings together all the systems, networks, data, processes, applications, and services that support business operations in a cohesive, resilient, and trustworthy manner.

The Information Assurance Technical Framework (IATF) used an interesting turn of phrase to describe Information Systems Security Engineering (ISSE). The IATF described ISSE as:

Information Systems Security Engineering (ISSE) is the art and science of discovering users' information protection needs and then designing and making information systems, with economy and elegance, so they can safely resist the forces to which they may be subjected. IATF, Chapter 3.

Engineering is a core element of building a reliable information security framework. If security has not been engineered into the processes, applications, networks, operating systems, and other aspects of modern business practices, it is unrealistic to expect that the networks will be able to resist attack or compromise without our assistance.

The description of ISSE as both an art and science is very accurate and meaningful. Information security requires both creativity and discipline; people and technology; prevention and correction; function and assurance, and policy and procedures.

The security manager requires to provide direction and focus during the engineering and architecture efforts so that security is integrated into the design and building of the information system. Security cannot be an afterthought or excellent option to have if time and budget permits. Security must be integrated into every business process and policy.

A central requirement for a security program is that it is led and managed correctly. This is the heart of governance, and effective governance is one of the primary demands placed on an organization today. The assets of the organization must be identified and protected. Senior management must actively work to understand the risk faced by the organization and create a culture of stability, accountability, and compliance. The security manager must work with the senior management team through reporting, recommendations, strategic plans, and demonstrating leadership in incorporating security into the organization's governance framework.

To many security workers, security is all about being busy. There are many demands on a security professional's time. There are never enough resources, time, or support to accomplish everything the security professional needs to get done. But a true professional knows that some of the most valuable time is when there is the opportunity to learn, explore, design, and discover. The security manager is not just another worker. She is busy juggling the demands on her time and setting priorities; she knows that planning is a crucial factor in efficiency, success, and long term sustainability. The security professional knows the value of a plan before building, thinking before doing, and having a comprehensive vision that goes beyond individual problems, individual systems, or immediate requirements. The security professional knows the value of engineering and architecture.

This book will look at the core concepts, practices, and objectives of a security program, and provide a comprehensive overview of the many areas of responsibility that a security professional must be familiar with.

Enjoy this book. You may not agree with everything. That is what makes our lives interesting, but hopefully, this book will make you think and consider opinions.

Never stop learning and growing, never give up on the fascination of youth and the potential of life. Enjoy your work, rise to the new challenges that every day brings and always work to make your world and the world of those around you a little bit safer, happier, and enjoyable.

CHAPTER 1: INTRODUCTION TO SECURITY MANAGEMENT

Information Security management is a relatively new field of specialization. Only in the past few years has it emerged as a core business requirement and demanded the development of a core team of professionals. They must have the skills and expertise needed to protect the information assets of the organization and know-how to manage information in a reliable, stable, and acceptable manner. The information security manager must be able to merge technology with business and balance risk with control and productivity. However, a manager cannot manage something that they do not understand and cannot find ways to integrate security into the processes of the organization. What if they do not have a thorough understanding of what risk is? What if they don’t have answers to questions like what is business and business priorities and strategy, what is technology, and how to understand and work with staff and customers? The information security manager must be part diplomat, part enforcer, part manager, and part user. The security manager must be able to build a bridge between different parts of the organization and forge the links between technology and business units that will provide security across the enterprise and throughout the organization.

The first challenge faced by an information security manager is to ensure that a common language is used to define security. Why it is crucial, and why security is an issue that every person in the organization is actually responsible for?

Yes, everyone is guilty. Some more than others, but the first step towards building the culture and the environment that creates ownership and personal accountability for the development and implementation of a comprehensive security program starts with the recognition that security is a part of everyone's responsibility.

Defining Information Security

If a survey asking 'what information security is' was to be conducted in your office, what would the results be? If each person, from the janitor that cleans the floor to the Managing Director, was asked what information security is, how would they respond?

To a person that watches a football or cricket match for the first time and that does not understand the rules, the game may only appear to be a lot of people running around in a disorganized manner and for no apparent reason. A person unfamiliar with the game does not understand the strategies and synchronization required to be successful, and they do not understand the crucial role that each player on the pitch actually serves. Such a person needs someone to explain the rules, describe the strategies, and point out the actions and procedures that lead to victory - or defeat. A football match is also an excellent example of a combination of short, mid, and long term strategies. A quick pass may provide some progress while the main goal is to score points, a few at a time (mid-term plan), to achieve a winning result (long term strategies).

The first challenge the information security manager faces is an incorrect understanding of what security is. This is because of the knowledge of what security varies widely from one person to another - especially between security professionals, managers, and users.

To the user, security is often perceived as:

- Passwords
- Pain
- Annoyance
- Slows down their work
- Guns or guards
- Someone else's problem

To a senior manager, security is often seen as a:

- Cost
- Liability
- Risk
- Technology

In fact, most senior managers are not convinced that protection really adds value to the organization at all. Instead, it is a necessary cost, and in many cases, they just hope that it is working. The average manager often believes that information security is something they are doing as best they can. But not at all sure that the security program is really working effectively or would be able to withstand a concerted attack from a team of skilled hackers.

What is information security to an information security professional?

In class, I often ask the security professionals what the term "security" represents to them. Even here, the answers vary widely. On a forum years ago, a security professional mentioned a challenge they had just faced. They stepped into an elevator on the 14th floor of their building headed outside for lunch and some fresh air. The elevator stopped on the 12th floor, and the managing director of the company walked onto the elevator. The director greeted the information security professional and asked kindly, "So, tell me, what do you do for the organization?"

This is a question we need to ask ourselves. As security professionals, what DO we do FOR the organization? We are parts of an enterprise - but only minor parts. We provide a service, but in the end, for most companies, we are not the department that actually generates revenue and profit. We are a cost - but are we a benefit?

The problem is that most security professionals would be uncomfortable answering this question. Why? If we do not clearly understand how to explain the benefit that we provide to the organization, then how do we expect that anyone else knows why we are needed? We need to be able to answer that question in a matter of seconds. We must be able to explain why we should still have a job after lunch. How can we use such a situation to win the respect and attention of management? Ideally, the Managing Director will be so intrigued by our response that he will seek further opportunities to meet with us and get a chance to ask us for details. In the end, too many security workers have found out all too quickly how easy it is for senior managers to consider a large part of the security team expendable once the organization faces budget cutbacks or re-alignment of priorities. Maybe this is in part due to the challenges a security professional often has in describing the value they bring to the organization and not being able to explain why having a dynamic and proactive security team can be a significant advantage to the business.

Security is a business enabler - we are a part of the business - an integral thread that should be woven into every business process and through every part of the organization. The security department is not an empire. Security was not employed to harass or punish users. Our job is not to spend our time treating the rest of the organization as enemies or adversaries. We are here to support, protect, and work WITH the business to earn their trust, gain their respect, and, most of all, obtain their cooperation.

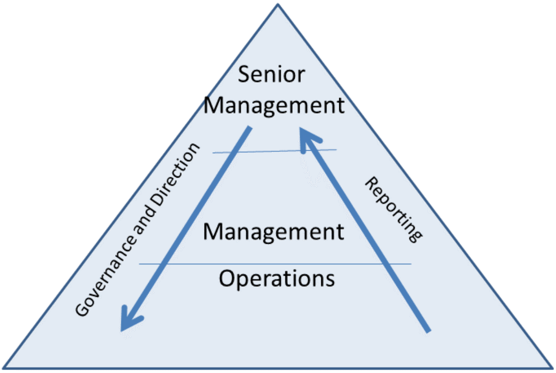
If you want to be a security professional, then you need to take this approach. The security professional is a strategist, architect, engineer, visionary, and planner. She knows how to get the most benefit from the few resources available and build a security program that is part of the business, closely aligned with the priorities and risk appetite of senior management.

Governance

Every few years, we see specific terms become a central part of our vocabulary. In the past few years, the word of choice has been "governance." (In recent years it was "prime," "enabler," or other such meaningless terms). Over this same period, there has been a lot of emphasis placed on governance, but it is surprising to see that many people still struggle to define what management is. Governance is based on the concept of oversight, responsibility, accountability, and ownership of an asset. IT governance is the responsible protection of the IT assets of an organization from harm. The purpose of IT governance is the principle of assigning and accepting responsibility for managing IT systems, hardware, data, networks, and monitoring systems. Without ownership, no one is responsible, and therefore, no one person can be held accountable for the safeguarding of the asset. If a group of people is trustworthy, then we often see that no one person is genuinely liable.

The recent past has been littered with examples of a lack of accountability and governance. Many organizations have committed fraud, failed to protect assets adequately, and disclosed personally identifiable information (PII) inappropriately. Several countries have passed legislation, and industries have developed standards in an attempt to increase accountability and personal ownership, for compliance with laws, acceptable standards, and best practices. These laws have various levels of effectiveness and often introduce a high cost to the organizations affected. A core principle required to protect the assets of the organization is to define the roles and responsibilities for the oversight and management of the security program.

The ultimate authority and accountability for the governance of the organization is the senior management team and the board of directors. They are responsible and accountable for ensuring that the organization follows the law, behaves ethically, and defines the level of adequate protection of the assets of the organization and levels of risk acceptance. Many of these principles (ethics, law, compliance, etc.) will be examined in more detail later in this book.



Governance and Reporting
Image #1

Establishing a Security Department

One of the first steps to good governance is to mandate the establishment of a Security Department to manage the security requirements of the organization and report back to the senior management team on the status of the security program. Also, to provide recommendations for future development of the security program, manage and report on incidents, and support or assist in monitoring, compliance and audit activities.

It is always a challenge to know who the security department should report to within the organization. Security, especially information security, is a newly emerging field and has not risen to a level of prominence that grants it a seat in senior management meetings in most organizations. The trend, however, is moving towards Security becoming an essential part of the management team and reporting directly to a senior manager. This reporting structure is critical to ensure that security has an enterprise-wide mandate and is not seen merely as a small, ineffective part of one business unit.

There is no perfect answer to the "who security should report to" dilemma. In many organizations, IT security reports to IT (perhaps to a Chief Information Officer (CIO)). Reporting to IT can seriously hinder the effectiveness and ability of the security department to enable change or force IT systems to be compliant with best security practices. This is because the IT department is primarily mandated to providing IT services, and IT security is seen as a hindrance to the business. If the organization has to decide between capacity and safety in cases where there is not enough time or budget for both, then security is frequently the loser.

Other approaches to the reporting structure for security have been to have a security report to Human Resources, Finance, Operations, or the position of Chief Information Security Officer (CISO).

Regardless of who or where the security department reports to, the role of the security department manager must be to learn how to be as effective as possible to build a security program and establish a culture of security into the organization. Being in an awkward position is not an excuse for not working hard to develop a security program that gains the respect of the other parts of the organization!

The security manager must build a team that has the skills, enthusiasm, and commitment to the function and purpose of security. Since security is a vast area, it is nearly impossible to find one person with all the skills needed to support all the tasks and investigations going on in Security. The security manager must be able to find liaisons within the departments of the organization that can promote and report on security issues within the user community and senior management. Outside experts will often be needed to provide specialized skills - forensics, interviewing, penetration testing, and audit. The security manager is often faced with low budgets, lack of support, and unrealistic expectations, but that is the challenge that makes a true leader excel. A security manager develops the staff required, does not rely on technical solutions to compensate for lack of procedures, and ensures that the security department develops an attitude of communication and accountability.

The security function is most often seen as a cost to the business, and the perception by most managers is that it hinders the operations of the company more than it helps. Additionally, security is a cost imposed on the business, but that provides little benefit. The security manager must demonstrate the value of IT protection and be able to justify the security budget. This is done through proper business case development and the use of project planning standards to outline the security objectives. The security manager must demonstrate how the purposes of security are aligned with business strategy, objectives, and goals, and how investment in safety will provide measurable results. The security manager should seek the approval of senior management of the security strategy. This is obtained through the communication of security requirements, legal requirements, best practices, gap analysis, and outlining a clear roadmap. The roadmap will provide milestones and deliverables that will track and report on the progress and status of the security program.

The security strategy must not be based on past events or a perception that future requirements will be an extension of the current ways of doing business. Just as the company is looking to evolve, so also must the security strategy be aware of new technologies, new business drivers, and emerging threats. The rapidly changing operational environment may result in operating conditions that are substantially different from current conditions. Since strategy is long term - with a focus on the future - the security manager must become a visionary that is looking at the world of the future when putting together a security roadmap. A security budget that is only aware of current or past issues will not earn the respect of senior managers that are focused on long term goals. This requires the security manager to talk with senior managers, listen to their perception of the future, and seek to develop a strategy that supports and enables new business initiatives.

Business Alignment

One of the essential responsibilities of the security professional is to design a security program that is aligned with the strategic direction of the organization. Business is always moving, and new technologies emerge. That can present new opportunities for the company. The company does not remain static, so the security program must also be flexible, forward-thinking, and creative. One of the most severe errors a security professional can make is to design a security program that provides solutions for yesterday's problems. The IT security program must align with the future direction of the business.

The security manager may not welcome the direction the business is going, (after all, security was much simpler 20 years ago in a centralized mainframe environment [with no internet] than it is today). Still, regardless of the desires of the security manager, it is the role of senior management to determine the strategic path and direction of the organization. The security professional is responsible for tying into and aligning the security program into the course of the strategic plan of the business.

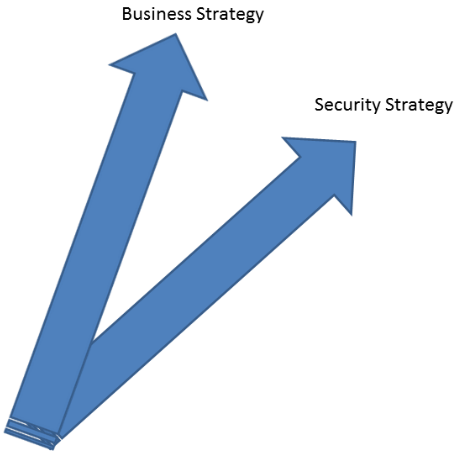


Fig 2 Two divergent roads showing security/business alignment

If security maintains a direction separate from that of the business, then security will become more and more isolated and irrelevant. The voice of security will become more of an unwanted annoyance like a dog barking at night than the sound of a watchman guarding the city. Security will bark at everything it sees or fears instead of being a partner and support for the business. Business wants to move ahead, try new technologies, and venture into new markets, and the role of the security program must be to support that development, not hinder it.

Missions and Goals

Every organization is different. The most obvious in organizations is the difference between a commercial enterprise and the military or a government agency. The military is interested in accomplishing a mission, a business enterprise in generating profit, and the government in providing service. Regardless of the type of enterprise, each kind needs security, and the role of the security professional must be to develop a security program. This program is tailored to that organization's priorities, culture, mission, and regulatory environment. The meaning of security for a commercial organization is tempered with the need to conduct careful cost/benefit analysis and to balance risk with opportunity. This becomes especially important as we examine risk and risk appetite later in this book.

Enterprise-wide Security

Most organizations are built in silos. They have separate departments - Finance, Human Resources, Sales, Manufacturing, etc. Each department is a separate entity - with its own leader, budget, staff, and business processes. IT and IT security are similar in that they are often independent and different from the rest of the organization.

In many cases today, we see that IT is even outsourced and provided by a separate company or agency (often as a service called "the cloud"). The "silo" mentality of business organization can lead to problems. However, an organization is made up of many pieces, but each of those pieces needs to work together effectively. A problem in one area is sure to have an effect on other areas.

Organizations are becoming more and more integrated with IT systems and processes that span many different silos. For example, IT systems span across departmental boundaries (Customer Relationship Management systems (CRM), and Enterprise Resource Planning systems (ERP).) This creates a new level of complexity since a breach or failure in one area will quickly lead to a problem in other departments or systems. Just like the human body, the body cannot ignore an infection in one place; today's IT is the same. Weakness in one system becomes a weakness throughout the organization. A breach in one area may quickly lead to a compromise in another department. We have even seen how a violation in an environmental control system (air conditioning) for a building could result in a breach of the organization's core IT and financial systems. The focus of security today must be on consistency - protecting everything as well as we can and being able to respond quickly and effectively whenever anything does go wrong.

This requires a new attitude and approach to both IT and IT security. IT and IT security are not just departments or silos - they are the basis and foundation on which most business processes run today. They must see themselves and be seen as a supporting function that is woven throughout the organization. IT supports every business department, interleaving data between systems, and providing consistent, measurable levels of risk management, structure, and direction to every part of the organization.

Some of the methods used to develop a security plan can include the SWOT analysis and the Balanced Scorecard.

SWOT analysis is a careful examination of the organization concerning its strengths, weaknesses, opportunities, and threats (SWOT). The organization needs to pursue its measurable, develop its opportunities, remediate its vulnerabilities, and be ready to address the risks it faces.

The Balanced Scorecard is a way to align business activities with the vision and strategy of the organization. This is done by examining the approach of the business from four contrasting perspectives; financial goals, learning and growth, the perspective of the customer, and the perspective of the company. By seeking a balance between the various aspects, the organization can develop a solid strategic plan that represents the vision of the organization.

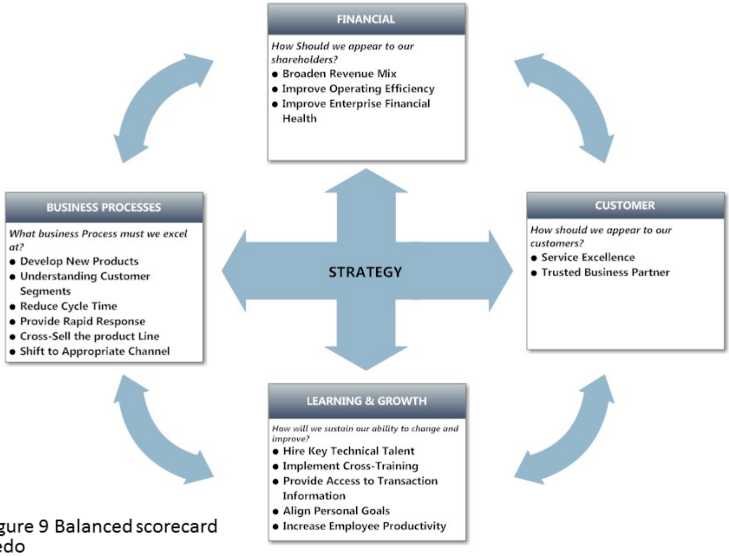

FINANCIAL
How Should we appear to our shareholders?
● Broaden Revenue Mix
● Improve Operating Efficiency
● Improve Enterprise Financial Health
BUSINESS PROCESSES
What business Process must we excel at?
● Develop New Products
● Understanding Customer Segments
● Reduce Cycle Time
● Provide Rapid Response
● Cross-Sell the product Line
● Shift to Appropriate Channel
STRATEGY
CUSTOMER
How should we appear to our customers?
● Service Excellence
● Trusted Business Partner
LEARNING & GROWTH
How will we sustain our ability to change and improve?
● Hire Key Technical Talent
● Implement Cross-Training
● Provide Access to Transaction Information
● Align Personal Goals
● Increase Employee Productivity

Figure 9 Balanced scorecard Redo

Adapted from the Balanced Scorecard by Robert S. Kaplan and Dave P. Norton. Harvard Business School Press. 1996.

Factors in Developing the Strategic Plan for Security

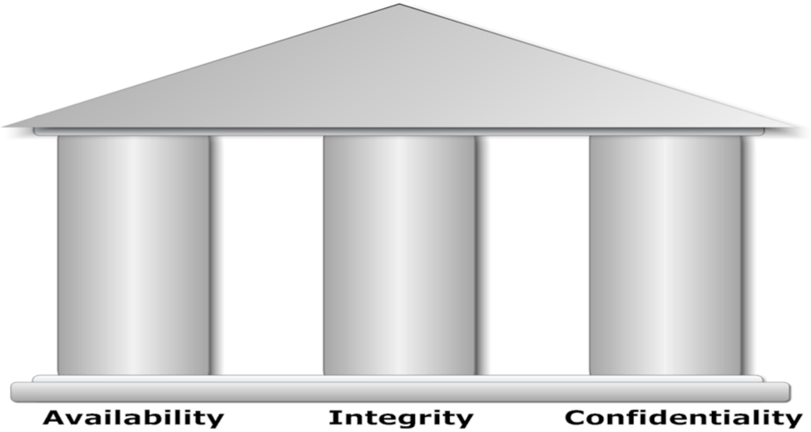
Many organizations are involved, supporting many lines of business, multiple facilities, operating in different regions or countries, and under various forms of regulation. The security plan of an organization is unique for each organization. The security plan reflects the culture and operating environment of the organization - whether it is very restrictive and highly regulated, or open and risk-taking.

In some cases, this even means having to develop a different security plan for different locations or departments. The security strategy must reflect the goals and objectives of the business and the senior management team. It must be legal and compliant with the laws and regulations the organization is operating in. A security plan cannot be restrictive when the culture of the organization encourages taking the risk. The program cannot be trusting and open in an organization that is cautious and conservative. In this way, the security manager must develop and implement a security strategy that reflects the goals and culture of the organization.

The Security Triad

As discussed earlier in this chapter, security is an abstract term that can be hard to explain, measure, or understand. Therefore, for many years, the concept of IT security has been defined using the CIA triad. This approach emphasizes security measurably and understandably.

Image #3 – the AIC Triad



Availability:

If we think of accessibility as a measuring stick (yardstick, meter stick), then the benefit of using availability as a way to define security becomes clear. A system may be available 100% of the time-continuous availability - or it may be available only a limited percentage of the time. It is up to the business to determine what level or rate of availability they require (and are willing to pay for). The level of dependence that the company has on the system is a measure of how "critical" that system is. The first challenge is to work with the business to "discover" what their availability requirements are. The company may not really know the answer to that challenge. They would like systems and data to be available ALL the time - but in reality, they usually do not REQUIRE that level of access. What happens during the lunch hour? Does anyone NEED the system then, or is it not required? Is the system more critical at certain times of the day than others? At month end more than mid-month? If the system that usually provides the data is not available, then can the critical data still be accessed in some other manner? Working with the business to discover their availability requirements is crucial to determining the level of availability we must aim for. Once we know the level of accessibility we desire, the target, we can build a plan to reach that target. But before we can write a plan or strategy to achieve a specific goal, we must know where we currently are. It is fine to know you want to enter a particular address on a map, but the secret to reaching that location is to understand where you currently are! (It does no good to plan a strategy to get you from Boston to New York if you are currently in Baltimore!). Now back to our yardstick.

Image #4 of yardstick

Once we have worked with the business to determine the level of availability the company requires, and we have examined the level of accessibility we are currently providing. We know whether or not we are meeting business requirements.

Remember, it does not matter what level of availability we want to give them - we are responsible for providing the level of service they demand. Once we know what we are offering, then we can develop the plan and strategy to address any gaps or shortcomings. However, more than once, when the IT security department measured the level of availability that they were providing, it was already more than the level of accessibility the business really required! This is a tangible benefit of measuring what security is - and the benefits it provides. For the first time, the company may realize that security is providing a measurable result and benefit by ensuring that critical systems are up and operating as required. This is a perception that is opposite to the users' common belief that systems are always down or unreliable. Now when management hears complaints about a system outage, they know that their information systems and security are working at acceptable levels of performance.

When the level of availability is not at the desired level, then it is possible to map out a strategy to move from the current level of availability to the desired level. This may not be possible in one step. A strategy that will move incrementally from the current level through various milestones and deliverables towards the desired objective may have to be defined. This gives the security and IT departments an advantage in that they can now justify their projects by linking them to measurable and achievable goals.

Confidentiality

Confidentiality is the protection of sensitive data from compromise or disclosure. In many cases, the requirements of confidentiality are in conflict with the goals of availability that want to make information available! Security is not about denying all access - it is about enabling the CORRECT level of access so that the person that requires access can efficiently perform their jobs. Confidentiality enforces the principle of the need to know. Confidentiality is also related to secrecy, the protection of personally identifiable information (PII), the protection of intellectual property such as trade secrets, and compliance with legislation and regulatory requirements related to the protection of information.

Confidentiality is often provided through encrypting data (rendering it unreadable) or masking the data - displaying only the last four digits of a credit card, for example.

Integrity

Integrity is a very important concept related to accuracy, precision, and trusted processing. Integrity ensures that data maintains a correct level of precision - is not changed improperly, cannot be tampered with, it is complete, and is therefore trusted. The integrity of systems refers to the correctness of processing, the accuracy of transactions, protection from malicious or accidental changes, and the principle of least privilege. Integrity can be summed up in three core rules:

1. Unauthorized users cannot make modifications
2. Authorized users cannot make improper modifications
3. Maintain internal and external consistency.

Protecting information from improper modification is accomplished by restricting users from making any modifications that would not result in the proper accuracy or consistency of the information. Any changes made to information must update all relevant systems properly and ensure that the data on our systems can be trusted. This is done through processes such as well-formed transactions and separation of duties.

A transaction is an operation on an information system, usually consisting of an input, a process, and an output. Since a large percentage of data contamination comes from invalid input, the first step to protecting the integrity of the data in our systems and the integrity of the processes that manage the data is to enforce checks and validation of data being input to the system. Input data may originate from users, customers, or other processes. The general rule is to trust nothing! Validate all input data to ensure it is consistent with the rules - within acceptable limits, values (alphabetic or numeric, special characters, or symbols). This will be the first line of defense against integrity problems.

The next step is to ensure that the processing of the data is correct - the right account is updated with the right amount! Arithmetic operations and calculations have to be checked to ensure completeness (no transactions were missed), correct addition, rounding, and storage.

Log the transaction in case a follow-up is needed - who made the change, what change was made, and when the change was made, sometimes even where the change was made from. The logs should also be protected so that a user is not able to hide or delete their activity. While processing data, the memory areas allocated to the process need to be re-initialized before re-use to prevent data contamination or disclosure.

The integrity of data may also be compromised during the output process if the data is not displayed correctly - the output field is too small, or the last transaction is not written to a file or report.

Several sources also advocate the inclusion of another part to the information security triad - the aspect of non-repudiation. To repudiate is to deny. This can be used when a person wants to refute or deny participating in a transaction or claim that a document has been altered. In a world of e-commerce and electronic transactions, it is vital to establish authenticity and a source of electronic transactions.

Summary of the CIA Triad

The CIA triad is an excellent way to describe the core principles of information security. It expresses information security in a way that can be understood by and is relevant to management, users, and other non-security personnel.

The Security Framework

All through this book, we make a small error. We refer to this field as IT security - Information Technology security. In fact, it would be more accurate to use the term IS Security - Information Systems Security. Security is much more than just technology. Security is a factor in every part of the business - processes, information, systems, networks, users, management, facilities, and applications. Security is a culture, an accessibility that requires structure, metrics, policies, enforcement, and support.

Setting up a security program starts with senior management support and a mandate that grants the authority for the security department to represent the interests of senior management in the establishment of policies and procedures that will address the security requirements management is seeking.

Use of a Framework

The use of a framework is an excellent way to ensure that the security program is complete and thorough. A framework provides a skeleton that can be adapted for use in many organizations, even in different regions of the world. The use of a structure that is internationally recognized may provide more assurance to auditors or reviewers. This often adds additional assurance that the security program is complete and did not miss any critical issues. Some examples of common frameworks are shown here:

ISO/IEC27002:2013 Information Technology - Security Techniques - Code of Practice for Information Security Management

The ISO/IEC27002 outlines best practices and guidelines for Information Security Management. It, like most other best practices in the information security field, is based on the principles of risk management. It outlines the requirement to assess and treat security risks through a risk assessment methodology that balances business risk with the cost or expenditure of controls to manage the risk of harm to the business.

The ISO/IEC27002 breaks controls into 14 security control categories with control objectives and 114 security controls that can be applied to meet the control objectives. The fourteen security control clauses are:

- Information security policies
- Organizing of information security
- Human resources security
- Asset management

- Access control
- Cryptography
- Physical and Environmental Security
- Operations security
- Communications security
- Systems acquisition, development, and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

Many organizations use the ISO/IEC standard as a template to build their own security program. It is a reputable and comprehensive list that allows the flexibility to adjust an organization's security program to its specific risk and business environment.

Organizations that want to be evaluated and certified as compliant with the ISO-defined information security best practices can be certified under the ISO/IEC27001 standard. That standard outlines the Information Technology - Security techniques - Information security management systems - requirements.

PCI-DSS - Payment Card Industry - Data Security Standard, Requirements and Security Assessment Procedures (version 2.0)

The payment card industry data security standard is an excellent template for the protection of sensitive information. This standard was written by a consortium of companies that issue payment cards (credit cards, debit cards, etc.). It is aligned with two other measures dealing with payment card security - the Payment Application (PA-DSS) and the Payment Card Industry Pin Security Requirements. These standards are a requirement for organizations that handle credit cards. The level of compliance with this standard that an organization must demonstrate is dependent on the number of payment card transactions dealt with by the organization per year.

Even though this standard is explicitly written for organizations that handle payment cards, the principles and practices advocated by this standard can provide an excellent foundation for a security program. This is true for any organization regardless of whether the organization handles payment cards or not.

The six main areas addressed in the PCI-DSSv3 are:

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

COBIT A Business Framework for the Governance and Management of Enterprise IT

ISACA's COBIT is another excellent tool that can be used to establish a comprehensive security program. The five core principles of COBIT 5 are:

1- Meeting Stakeholder Needs
2- Covering the Enterprise End-to-end

3- Applying a Single Integrated Framework
4- Enabling a Holistic Approach
5- Separating Governance from Management

COBIT is supported by several other documents and standards that provide guidance to the team implementing a security program. These include the Professional Guides: COBIT for Implementation, COBIT for Information Security, COBIT for Assurance, and COBIT for Risk.

NIST

The NIST Special Publications are a wealth of excellent information for the Information Security Professional. NIST (National Institute of Standards and Technology) provides the standards and guidance documents for use in the U.S. Federal Government through their website *http://csrc.nist.gov*. NIST recommends that its standards be implemented by all types of organizations. All of the NIST special publications can be accessed at no cost.

Here are some examples of relevant NIST documents:

NIST SP800-53 Recommended Security Controls for Federal Information Systems

NIST SP800-53 outlines the recommended security controls for information systems based on the security categorization of the information and the information system. The classification of the system is based on the impact level of a breach of availability, integrity, and confidentiality (the CIA triad). Depending on the security categorization of the information system (Low. Moderate or High), SP800-53 lists what security controls would be recommended.

NIST SP800-100 Information Security Handbook: A Guide for Managers

NIST SP800-100 outlines the primary areas of concern for Managers. These include:

- Information Security Governance
- Systems Development Life Cycle
- Awareness and Training
- Capital Planning and Investment Control
- Interconnecting Systems
- Performance Measures
- Security Planning
- Information Technology Contingency Planning
- Risk Management
- Certification, Accreditation and Security Assessments
- Security Services and Product Acquisition
- Incident Response
- Configuration Management

Summary of Frameworks

Each of these frameworks can be a valuable tool in the hands of the security professional. Just like a recipe to a chef, these frameworks can help ensure that nothing is overlooked or missed in the creation of the security plan. It also provides that the program will be authoritative, balanced, complete, and justifiable.

It must be remembered that the use of a framework is not a guarantee that the security program will be ideal or successful.

For that, you also need alignment with business priorities and senior management support (among other things like awareness training, excellent staff…), but the framework can help.

Policy

One of the priorities and deliverables of an information security program should be the creation and approval of information security policy. The plan is the core document that outlines the boundaries, objectives, and authority of the information security program. Without a plan signed by senior management, a security department lacks the credibility and authority to investigate or enforce security practices and principles.

It is common for the security manager to have to write the policy and then send it out for review, adjustment, and finally, approval. The plan is approved by a senior manager (often the Managing Director or Chief Executive Officer) and then distributed to all areas of the organization that it applies to. A policy reflects management's intent and direction and mandates compliance with laws or standards.

A policy document should be short, clear, and easily understood. It should be written in a way that is not technically constrained and would, therefore, be quickly outdated as technology changes. The Information Security policy must be legally enforceable and aligned with the culture of the organization and other organizational systems such as Human Resources and Health and Safety policies. The plan should have an owner that is responsible for annually reviewing and updating the project when needed. Every policy should allow for enforcement and disciplinary action if required and have a formal process for exception handling.

A policy should always indicate the scope of the plan, including who it applies to - which should, of course, include employees, temporary employees, contractors, third party business partners, and managers.

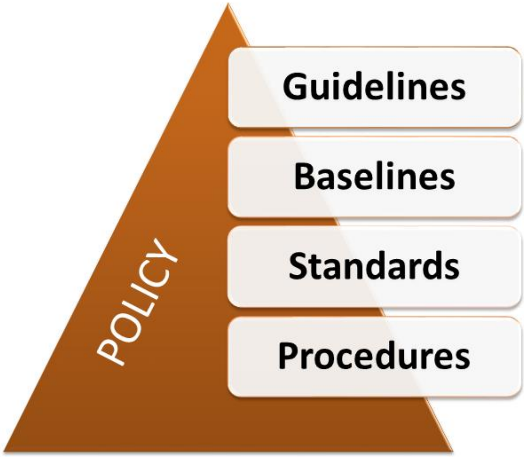
Having a policy that sits on a shelf is a common problem. The plan must be communicated to all staff and other relevant parties to be effective. The program should be available for reference and a crucial part of awareness sessions and annual job performance reviews.

We casually use the word 'policy' as if it is one document, but there are many policies for an organization. The core policy document is often short, high-level, and rarely subject to change. However, the core policy is implemented and supported by numerous functional policies that address individual issues and technologies. Examples of these operational policies can be a remote access policy, acceptable use policy (describing fair use of the internet or other organizational resources), incident handling policy, anti-virus policy, etc.

The Interpretation and Implementation of Policy

A policy document, even when signed and endorsed by senior management, is still only a collection of words and phrases on a sheet of paper. A policy is a foundation for the security program, but it is not enough. The policy must be interpreted into plans and strategies and implemented into action. The policy is achieved through the use of Procedures, Standards, Baselines, and Guidelines.

Image #5 – the interpretation and implementation of policy



Procedures

The policy is words, and methods are actions. Procedures outline the steps and activities that must be taken to ensure that core business activities are performed consistently, in the same way, each time, and so that any deviations or errors can be noticed quickly. Examples of procedures are a process to set up new user accounts, or a change management process. The latest user account process ensures that user accounts are only set up with proper permissions, set up correctly in a conventional manner, and are subject to review and validation. This reduces the chance of errors, social engineering, and inconsistent account management. By having a defined process that must be followed to set up a user account, accounts will be set up the same way regardless of which person actually sets up the account. By having a change management process, the organization has control over changes and can ensure that all changes have been formally reviewed, approved, tested, documented, and implemented correctly.

The use of consistently enforced procedures allows for the rapid detection of any events of non-compliance. A process should be practical, based on sound business and security requirements and not impede the natural flow of business. Outdated or cumbersome systems will frequently be bypassed - leading to a loss of credibility for the authority and necessity of the systems and management processes. Methods must be seen as mandatory, not just optional ways to implement the intent of the policy.

Standards

Standards, like procedures, are also used to facilitate compliance with the policy. A standard for tools, applications, platforms, and elements used within an organization allows the organization to control what types of devices and applications are connected to the corporate network and simplifies the purchasing, training, maintenance, patching, and configuration of systems. The use of standards may integrate with licensing systems that control the number of users and licenses available for proprietary software. Without having standards, the maintenance of systems and equipment may be very costly and challenging. The help desk would need to learn how to support multiple systems, carry various types of replacement equipment, and struggle with inconsistency between rules, configurations, and patch management. The costs of purchasing hardware or software may also be higher if purchases are not made on a bulk or preferred supplier basis. The prices of training users on multiple systems may also be higher, and make it difficult to move staff between departments that are using different equipment.

Standards provide benefits but also come at a cost. The enforcement of a rule may be seen as inflexible for parts of the business. That would be like the option of choosing their own solution or purchasing an application better suited for their local needs or to support local businesses. In the world of Bring Your Own Device (BYOD), this is becoming increasingly difficult to manage. Many users want to use their own, non-standard, and often uncontrolled devices.

Another risk associated with enforcing a standard for equipment or software may be the vulnerability of relying on one vendor. That could increase the chance that a breach or problem with that vendor may expose the entire organization to a potential threat.

Baselines

A baseline is usually described as the requirement for a standard configuration. The organization may have a required baseline configuration. That baseline may mandate that all devices that connect to the organization's network have an up-to-date anti-virus product. By setting out a benchmark for all devices that relate to the organization's network, the organization can better control the risk of malware. Many organizations have found that it is preferable to set mandatory thresholds or baselines for machines and software that is connected to corporate systems or networks. If the organization has required a personal firewall for each laptop, it may need specific rules so that every device that links will be secure. Usually, the baseline is a minimum requirement so that no equipment is allowed to communicate at a configuration lower than the benchmark.

Guidelines

As compared to policy, procedures, standards, and baselines (which are all mandatory requirements), instructions are recommendations. A guideline is a suggestion often of how to be compliant with necessary provisions. Guidelines may suggest how to create a secure password, or they may recommend how often to check for updates to anti-virus signature files. Instructions may be used to advise how to select products for purchase or what to look for in a review of system operations or processes. Guidelines provide answers to questions, advice on how to comply with requirements, and make security "simple" and understandable for users. An excellent example of the role of guidelines is the relationship between ISO/IEC27001 and ISO/IEC27002. ISO/IEC27001 is a certifiable standard that outlines the requirements for an Information Security Management System. In contrast, ISO/IEC27002 is a Code of Practice, a guidance document that describes the controls an organization could use if they wanted to be compliant with ISO/IEC27001.

Roles and Responsibilities:

Ownership

Earlier in this chapter, we discussed the role of senior management as the primary and ultimate authority for the protection of the assets of the organization. We know that senior management must support the establishment of a security program through the designation of a person responsible for security. Without someone "owning" security, then security simply does not happen. Security is not something that comes naturally to an organization - it must be purposely and intentionally built into the business processes. Security is like an ingredient in a recipe - if an element is left when the cake is being prepared, then that component is simply not there. The finished product will be tasteless or incomplete, and there is no way to quickly correct the problem of a missing part once the cake is baked. Security is provided through a conscious effort and must be appropriately measured, controlled, and added into the batter in such a way as to become a part of (integrated into) every area of the business.

The Security Manager

The security manager is the person responsible for leading the security program. The security manager must be familiar with local laws, standards, the culture of the organization, and best practices in the industry. Ideally, the security manager should be certified and have formal education in the field of Information Security. Information security is a broad field and few, if any, people have experience or familiarity with all areas of information security. Through experience and training, many security managers are firm in certain areas - perhaps they came from an application development area or a networking background. Then they are very comfortable with those areas of security but may have no experience in Legal, Business Continuity, or Cryptography. To be an effective security manager, they must gain knowledge and experience in all areas of security. Security is not adequate if it is only focused on networks but is weak in applications. Security must be woven through all departments of the organization, as described earlier. It must also be integrated into every level of the organization and each system. Excellent network security cannot compensate adequately for application flaws, hardware failures, or lack of training of users.

The security manager plays a crucial role in defining the security strategy for the organization, managing the security team, administering the budget, tracking the security projects, and reporting to management on the status of security controls, incidents, and compliance. The security manager sets the tone for the security department and must ensure that all security personnel is trained, doing their jobs competently and legally and that all incidents are investigated and resolved accurately.

Security Officer

The security officer works under the direction of the security manager within the Security department. Most of this book will deal with the responsibilities of the security officer - a professional that is instrumental in designing, implementing, monitoring, and enforcing security controls and assists with educating managers and users in security concepts and procedures. A security officer is often the prime person to manage an investigation into a security incident or user malfeasance. This requires the security officer to be extremely ethical, honest, thorough, and committed to protecting the confidentiality of an investigation. Many investigations may require the use of skills that a security officer may not have. This would need the employment of experts that can provide the advice and skills needed to investigate the incident accurately.

Physical Security Personnel

Physical security is the most visible element of the security infrastructure. Physical security personnel play an essential role in protecting buildings, managing access, and responding to physical security incidents. Physical security personnel are often subcontractors or supervised by a shared service provider that provides physical security services to many tenants in a building. An organization should ensure that physical security personnel can be trusted, are doing their jobs properly, and are enforcing the access control rules according to the procedures they have been given. All too often, an organization has found that the physical security they were paying for was not adequate. Security personnel are subject to social engineering or are lax in enforcing the rules. Security personnel should be adequately trained in how to deal with incidents.

System Owner

The system owner is one of the most important but poorly understood roles in the security program. This stems from the misconception that IT "owns" the IT systems and data that the organization uses. That is an incorrect understanding. The IT systems are "owned" by the business unit that pays for and relies on them. For example, a finance system that handles accounts payable or manages the general ledger of the organization is not "owned" by IT - it is owned by the Chief Financial Officer (CFO) or a person in a similar role. The system is supported by IT, and IT (whether outsourced or provided internally) is expected to manage, operate, and secure the financial system on behalf of the owner. The business owns the system - they pay for it, and they rely on it. The organization indicates where changes are needed, and they have the final say in when and what changes may be made to the system. As part of responsible management, the IT department will indicate when patches or upgrades may be needed, they may apply to the business for a time to shut down the system for hardware or network maintenance. Still, IT should never make a change to a system without the consent of the owner of that system. Just like a car, when you purchase it and take it to a repair shop - the mechanic may indicate work that should be done, but the mechanic is not authorized to perform that work without the permission of the owner of the vehicle. In short, a system owner is a senior person from the business department that relies on the system and pays for it.

The role of the system owner is critically essential. The system owner must decide who gets access to the system. The system owner must determine what changes should be made, when the changes can be applied, must monitor the reports on system controls. The system owner must ensure the network is being operated following the law, policy, and requirements of the information owner and possibly an authorizing official. The role of the system owner is an integral part of the security framework. Each system must have an owner, and the security administrator must ensure that access is only granted to the system following the mandates of the owner.

The challenge comes when the system owner is not aware of the security requirements they are accountable for. An owner may wish to implement as little security as possible since it may affect productivity. However, the system owner must realize that it is their responsibility to accept the risk of any resulting security breaches. For this reason, we see some movement in governments and organizations to declare a separate role of authorizing officials. The authorizing official has an enterprise-wide responsibility and operates at arm's length from the system owner. The authorizing official must approve all system changes or implementations before implementation. This ensures that no owner can put a system into production, operate an order, or make changes to a system that may pose a risk to other systems, the organization, or its operations. This is addressed through a process known as systems authorization or formerly known as certification and accreditation.

Information Owner

The information owner is the person designated to be responsible for the protection of the information held by the organization. Organizations are responsible for adequately protect any sensitive information they process, store, or transmit. The requirement to safeguard information applies to personally identifiable information (PII) intellectual property or trade secrets.

One of the first responsibilities of the information owner is to identify and classify all information being held by the organization. The process of information classification will be examined in more detail later in this book.

The information owner must ensure that information that requires protection is adequately protected. That means only authorized personnel can access that information, the data is being correctly backed up, and the data is destroyed when no longer needed. It also means that the data can only be changed through a controlled process.

Going back to the integration of many departments of the organization, we see that information that is gathered by one department may soon be transmitted or available to another department. This demonstrates why the role of the information owner is enterprise-wide instead of department-wide. The system owner is usually from one department and only has responsibility for the systems in their department. The information owner has the responsibility to protect data that may end up on several networks in more than one department. The burden of the information owner is to ensure that sensitive data is protected no matter where in the organization it goes. The information owner is the person who must accept legal responsibility for protecting that information and possibly facing some form of criminal or civil charges if the information is breached. This means that the information owner must be a senior manager and must have the authority to mandate how a piece of data will be gathered, stored, accessed, and transmitted. This includes when data is deleted regardless of what systems or departments the information belongs to. This includes when information is shared with business partners or handled by a third party. How this works in practice is that the information owner declares what information is protected and how it is to be processed. For example, a credit card number may be collected on a sales system but subsequently stored on a financial system or in a customer database. The information owner must mandate whether the information must be protected while being stored or transmitted (encrypted), accessed, deleted, and displayed (masked). Each system owner that processes, stores, or transmits that credit card data must agree to follow the mandate of the information owner. The system owner must be willing to enforce necessary protections on that data according to the order of the information owner. The information owner must have the authority to refuse to allow that information to be available to the sales system or department. Through this, we see the enterprise-wide mandate of the information owner. This is one of the most challenging aspects of information protection - especially given the many different laws and regulations about the handling of information. Sometimes the rules for handling data are different from one country to another or one industry sector to another, and the information owner or owners must be able to adjust to those various laws as much as possible.

Custodian

The role of the custodian is to have cared for, or custody of, an asset. The custodian of a sports trophy (ex. the Stanley Cup for Ice Hockey) is not the owner of the Cup but is tasked with the responsibility for the protection of the Cup - the secure handling, storage, transportation, display, and engraving of the trophy on behalf of the owner. This is the same as the role of IT. IT manages, cares for, operates, and repairs the systems of the organization on behalf of the system owners and information owners. IT has a level of access to information that no one else has, but with that access comes the responsibility to behave in a legal, ethical manner and not misuse, disclose or modify that data or system in an unauthorized way. There are far too many examples of IT staff reading emails, accessing customer data, or divulging sensitive information to unauthorized personnel. In some cases, the IT staff was not even aware that this was a violation of the law, company policy, or ethics. The IT staff erroneously thought that since they had access and managed the email system (for example), that they were entitled to read emails as part of maintaining the system.

This is an important distinction - the gap between ownership and custody. IT maintains the systems on behalf of the owners, and no changes should be made without the knowledge and consent of the owners. Even vendor patches to an application should go through a formal approval process before being implemented. A practical example of ownership is the current movement to put IT services on the "cloud." The business can decide to outsource their IT services and function and disband their entire IT department. This shows in a genuine sense how much ownership IT really has over the systems and technology of the organization.

Users

Users are the reasons that we have IT systems!! As much as users can be a problem, risk, and source of many issues, the systems are built for the users to accomplish their tasks and get their job done. Users need to understand and follow the rules, policies, and procedures of the organization. Users must know who to call or report to in case they encounter any system issues or problems. Users need regular training and awareness sessions to ensure that they are aware of corporate policies and procedures, and that they know how to use the systems correctly.

Local Managers

Security is everyone's business, but a critical factor in creating a culture of information protection and the enforcement of security principles is the role of the regional managers. Local managers have the day to day interaction with their staff. They are in the best position to notice any security issues and remind everyone of the requirement to follow security procedures. Following security procedures must be seen as an absolute, mandatory requirement - not merely a suggestion or optional activity. Local managers are the people in the best position to enforce this. However, most local managers only see themselves as business representatives and focus on their functional role in business activities. They frequently see security as the responsibility of another department and perceive the security group as "friendly enemies" that are more interested in stupid rules and procedures than in supporting their department's requirements. This is an attitude that needs to change. Local managers are accountable when there is a security violation where a user in their department is allowed to ignore security procedures. In the end, it is the local manager that is one of the most important members of the security team and therefore needs to understand the role and reasons for security in their area of responsibility. More and more organizations are moving in the direction of continuous auditing and control self-assessment. These approaches require the local manager to be more involved in designing, monitoring, and reporting on security controls and measuring the effectiveness of those controls. The security team also needs to work with the local managers to ensure that the security procedures and policies are reasonable, up to date, and relevant.

Auditors

Auditors are an essential part of governance. Auditors are responsible for reporting to management on the status of the controls in place to protect the systems, processes, and operations of the organization. Some auditors specialize in financial audits, others in operational or IT audits. Regardless of which areas are being checked, however, IT is almost always involved since nearly every system or business process today has some IT component. Auditors are to be independent, objective, and systematic. They are expected to investigate, discover, and uncover any flaws or vulnerabilities in systems, and report on any areas of non-compliance with organizational policies or procedures.

Auditors are the eyes and ears of senior management and are expected to develop and follow an annual audit plan that focusses on the areas of most concern to management. Through proper examination and evaluation of systems and processes, auditors provide management with findings and recommendations on how to improve processes, strengthen controls, provide better oversight, and increase efficiency or effectiveness.

IT staff are often required to provide support for audits, and this can take a considerable amount of time. However, a properly conducted review may be of significant advantage to an IT department. Issues that may have been challenging for the IT or security department to resolve may be highlighted in an audit report and (finally!) receive the attention and budget required.

Third Parties, Vendors and Contractors

Everyone that accesses or works on the systems, networks, facilities, or data of the organization must be subject to the rules and procedures of the organization. This is especially challenging in a world of outsourcing. As organizations outsource their data processing, applications, or some business processes, the need to ensure that the service provider meets the security and data protection requirements. It must be remembered that when an organization accepts, processes, transmits, or stores sensitive data, then that original organization remains liable for the protection of that information even if it is shared with another service provider.

Roles and Responsibilities Summary

Security is the responsibility of everyone in the organization. Adequate protection can only happen when everyone is aware of the need for security and realizes how their actions can affect the stability, resilience, profitability, and success of the organization. Security is not a "nice to have" or an option. It is a thread that must be woven into every business process, into the mindset of each person and integrated into each system and IT function. This requires a continuous effort of education, reminders, monitoring, and improvement. When everyone sees that the organization is serious about security and is committed to ensuring that the policies and procedures are being enforced, then a culture of security is created. At this point, each person will realize the importance of their role on the security team.

Security Metrics

The security department, like all other departments of the organization, must be held accountable for their budget, deliverables, and results. Security metrics are necessary to ensure that senior management can demonstrate governance and see into the workings and effectiveness of the security department. A failure by the security department to adequately protect the assets of the organization, including information systems, data, personnel, and equipment, may expose the organization to extraordinary risks, including financial liability, loss of market share, and even criminal charges.

Establishing meaningful metrics for security is a challenge. Metrics must measure the 'right' things, provide an accurate overview of critical functions, and be relevant to the needs of the organization. There is no sense in measuring items such as the number of types of malware that were discovered around the world in the past year - that is not an item that can be controlled or affected by the security department. Instead, the metrics should review measurable factors such as the speed at which a new breach was detected or an incident closed off.

Development of Metrics

There are several useful approaches to developing metrics for security. The first is the use of SMART metrics, as introduced by Peter Drucker. The definitions of SMART have changed over the years, but this is an excellent tool to ensure that the parameters that are being measured are appropriate for the organization. Here is one example of the application of SMART.

SMART; Specific Measureable, Attainable, Relevant, Timely.

Specific metrics are metrics that review a clearly defined process with defined objectives and thresholds for performance. An example of a particular parameter would be network availability. The business can set a performance objective of 99% availability. This is a specific, measurable value that would indicate either acceptable or unacceptable performance.

Measurable metrics are those that can be quantitative, objective, and detailed. Such parameters are numerically based (quantitative), not subjective, repeatable, and accurate.

Attainable - the metrics should be realistic and achievable - the parameters should not attempt to reach a standard that is simply impossible to achieve. If the business cannot reach the required level of performance, employees may stop trying since success is not possible. For example, an objective of 100% uptime would discourage the staff instead of inspiring.

Relevant - There is little value in measuring things that merely make management shrug their shoulders and wonder why we measure such things. The choice of what to monitor should be taken in consultation with management to ensure that the metrics are aligned with business priorities and management's interests.

Timely - is ensuring that the metrics are useful. If a metric reports on an event that has already long passed and where there is no opportunity to learn from the 1report, then the metric is of little use to the organization.

SMART metrics are only one of the ways that parameters are defined. There are many others, but the most important thing to remember is that parameters should only be used to measure issues that are relevant to the organization. These essential bits of data provide meaningful data that can alert management to the health and effectiveness of the information security management program. Goals must be aligned with legal and regulatory requirements, be accurate and repeatable, be objective, not subjective (subject to the preferences or personal interpretation of the auditor), and monitored. It is far too common to find that organizations have mechanisms in place to monitor their networks, applications, and other assets. However, after additional analysis, we see that no one is tasked with reviewing the controls and ensuring that regular reports are provided to management.

Another issue, of course, is where alerts and reports do indicate a problem; no one takes measures to correct the problem.

Indicators

Indicators are an essential part of metrics. A metric has no relevance unless it is related to a specific objective. These objectives may be based on many things, such as a benchmark. For example, par in a golf game is a benchmark that permits a person to know how well they are performing compared to a commonly accepted level of performance. Many organizations use parameters based on what other organizations in their industry sector or country/region are doing. Other indicators are based on regulations or on industry-specific standards such as the payment card industry (PCI).

ISACA defines a Key Goal Indicator (KGI) as a measure that tells management, after the fact, whether an IT process has achieved its business requirements. This is usually expressed in terms of information criteria. A key goal indicator can be used to demonstrate compliance or the success of a project such as a KGI that notifies management that a defined standard was met. For example, a business continuity test completed successfully.

A Key Performance Indicator (KPI) is defined as a measure that determines how well the process is performing in enabling the goal to be reached. A KPI is often the absolute requirement that must be met. For example, a company may need to ensure that security patches must be deployed within seven days of release and, therefore, set seven days as the KPI. Not to meet those criteria would be unacceptable.

A Key Risk Indicator (KRI) is defined by ISACA as A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating substantial risk. KRIs are essential indicators that would alert management to a potentially developing danger. For example, if an organization has set a threshold that requires all patches to be deployed within 7 days of release, that would be a KPI. A KRI may be configured to 6 days - that would alert management that the patch management process is close to being non-compliant and exceeding the KPI. Hopefully, the organization would then be able to take corrective action before the procedure is non-complaint, and the time taken to deploy patches exceeds the KPI.

Implementing the Security Program

Information security is one of the essential parts of a successful business today. A breach of sensitive data, or unreliable systems, can cause business interruption, loss of customers, and financial penalties. The organization must, therefore, have a security program - a vision, objectives and goals, personnel, tools, policies and procedures, and education and awareness programs.

The most fundamental requirement for a security program to be successful is senior management support. Without that support, the security program will be unable to influence, direct, and enforce security practices. Top management support will provide budgets, access to personnel, authority, and credibility for the security program. A security program will affect business operations and will result in having to change some business practices, even though it may impact productivity or performance. The security manager must be able to develop and design a security program that reflects business priorities and has the tact and skill to educate the personnel of the organization by convincing them of the need for security and their personal responsibility for following security procedures.

A security program will often be comprised of many individual projects and initiatives. It is vital to encourage the development of an enterprise-wide security architecture. Security should not be based solely on personal projects or applications since the result may be many different solutions with no interoperability - this lack of integration and loss of the ability to leverage existing components.

Summary of the Introduction to Information Security Chapter

This chapter sets out the foundation for an Information Security Program. This chapter addressed the core principles that the rest of the security program is based on: Senior Management Support, Defining roles and responsibilities, and the Creation of policy, procedures, baselines, and standards. These principles are based on the effort of the security professional to obtain support through clearly defining what information security is, making it measurable, and aligning security to business mission and strategy.

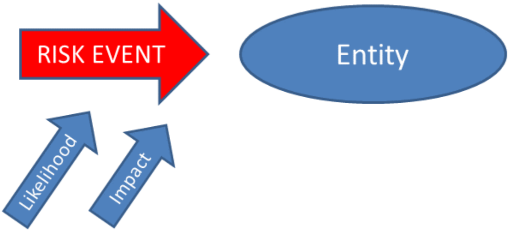
CHAPTER 2: RISK MANAGEMENT

Risk Management

Risk is defined in the NIST Special Publication 800-30 Rev 1 as:

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the situation or event occurs; and the likelihood of occurrence.

Image # 6



Risk is the Function of Likelihood and Impact of a Risk Event on an Entity

Risk is a measurable level of the potential impact on an asset due to some event, whether the event is accidental or intentional, regardless of the source, and dependent on the value of the entity or asset.

Risk Management is the science of managing risk in a cost-effective, justifiable manner. Risk management is comprised of three significant elements: Risk Assessment; Risk Response; and Risk Monitoring.

Risk

Risk is a function of the business. Risk is an integral part of managing the opportunities and threats that an organization faces. Without managing and accepting a certain level of risk, an organization has few opportunities to earn a profit or expand. However, uncertainty also places the organization in jeopardy of failure and economic collapse!

A bank uses the opportunity to lend money to make a profit. However, giving money to people with excellent credit ratings is a low-risk transaction and may only provide a relatively flat rate of return. If the bank tries to lend money at a high-interest rate to a good client, then the client may go elsewhere to borrow money. If a client with a mediocre credit rating tries to borrow money, the bank may be able to charge a higher interest rate. This allows the bank to make more profit on the money it lends out, but it also presents a higher level of risk that the client with a less than ideal credit rating may not be able to repay the loan. In that case, the bank may lose the money it lent out. In cases where a client has abysmal credit, the bank may choose not to loan money to the client at all. That means that the bank is not at risk of losing the money it would have lent out, but it also means that the bank loses the opportunity to make any money on the transaction.

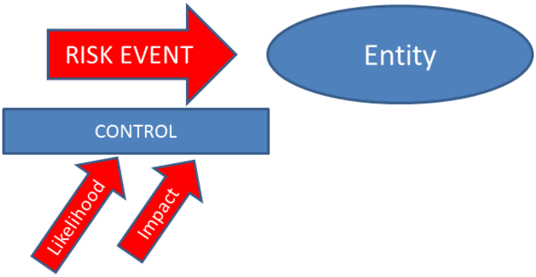
These are examples of risk management. The risk to a bank means opportunity but also potential loss. Refusing credit to a poor customer is an example of the risk response methodology known as risk avoidance. Loaning money to a client is an example of risk acceptance. Lending money at a higher rate of interest or requiring the client to provide collateral to support the loan is a form of risk mitigation. Re-insuring the loan with other lending firms or spreading a jumbo loan across multiple lending firms is a form of risk transference.

Risk management, therefore, is not just about avoiding risk. It is about managing risk by assessing risk, evaluating the level of risk, determining what would be an acceptable risk level, and then continuing to monitor the threat once it has been accepted. Any changes in the risk level should be identified as quickly as possible - and perhaps mitigated through new controls or countermeasures.

Controls

The response to risk is control. Controls may be technical (tools - anti-virus, password-based access controls), managerial (policy, Human resources practices), operational (procedures), and physical (locks). Controls may also be known as safeguards (proactive) such as awareness training and countermeasures (responsive) such as incident management.

Image # 7 Risk and Control



The Purpose of a Control is to Reduce the Impact or Likelihood of an Adverse Event Affecting the Asset or Entity

Risk Versus Control

The purpose of control is to address a specific threat. However, a control is also a limitation because are indirect costs for the purchase or installation of the protection mechanism. Therefore the selection of control requires diligence and careful consideration of the justification for the protection mechanism; The effectiveness of the protection mechanism, the impact on business, acceptance by the users, and the ability of the protection mechanism to support compliance or audit needs.

Therefore all controls should be justified by the risk that requires the implementation of the protection mechanism. The protection mechanism should also be traceable back to the threat to demonstrate that the protection mechanism is appropriate for the risk that the protection mechanism was designed to mitigate.

A control that cannot be tracked back to a defined risk is unnecessary, and a chance that is not adequately addressed through a command is a potential liability.

Types of Controls

Controls are usually either preventive or reactive. Preventive control is one that attempts to stop an adverse event from occurring, while reactive power is one that responds to a contest.

Preventive Controls

There are several types of preventive controls - directive, deterrent, and preventive.

Directive Controls

Directive control is a control that mandates the behavior of personnel. A policy that tells users what they can, or cannot do, is a type of directive control. An example of this would be an acceptable use policy. Other directive controls would be a sign that warns of "No Trespassing" or a warning banner shown to the user when accessing a computer system.

Deterrent Controls

A deterrent is a control that attempts to discourage a user from doing something wrong. An example of an obstacle would be a warning sign stating, "Shoplifters will be prosecuted," a clearly visible security camera, or a well-communicated disciplinary policy.

Preventive Controls

Preventive control is the next step in the control infrastructure. Even if a person is not deterred from doing something wrong, the preventive control will attempt to prohibit or prevent improper activity. An example of a preventive control would be a fence, a lock, a password requirement, or a strictly enforced change control procedure.

Reactive Controls

Despite the many attempts made to prevent an adverse event from occurring, it is still required to be prepared for intentional, accidental, or circumstantial events. This is where reactive controls such as detective, corrective, recovery, and compensating controls are used.

Detective Controls

Detective control is one that "detects" or notices an event with the intent to alert the organization and allow an adequate response. Examples of detective control are an Intrusion Detection System (IDS), a smoke detector (fire alarm), or a regular balancing of output and input transactions.

Corrective Controls

A corrective control is a control that attempts to "correct" or respond to an incident with the intent to regain control of the event and minimize the damage the development would cause. Examples of corrective power would be a fire suppression system, apprehending a suspect, or isolating a network.

Recovery (Restoration) Controls

Recovery controls are designed to restore a facility, a business process, or systems back to normal. The corrective fire suppression system put the fire out - and stopped the incident from spreading, but everything is certainly not back to normal after the light is out. The next step requires a recovery or restoration effort to clean up the damage, rebuild, and restore operations to normal. Other examples of recovery controls could be repairing a system from backup files, or training new staff.

Compensating Controls

Compensating controls are used where other controls are not available or are inadequate to protect the organization. Compensating controls are put in place to make up for (or offset) the lack of other restrictions. Examples of compensating controls are increased supervision of staff with elevated permissions, dual control or separation of duties, and cross-training of a team.

What is Risk?

Here are several definitions of risk from authoritative sources:

Risk is a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the incident. ISO/IEC 27005

Risk is a combination of the probability of an event and its consequence ISO/IEC 27002

The possibility that a particular threat will adversely impact an Information System by exploiting a specific vulnerability. CNSSI 4009

The NIST SP800-30 described IT Risk in this way:
IT-related risks arise from legal liability or mission loss due to —

1. Unauthorized (malicious or accidental) disclosure, modification, or
destruction of information
2. Unintentional errors and omissions
3. IT disruptions due to natural or man-made disasters
4. Failure to exercise due care and diligence in the implementation and
operation of the IT system.

As can be seen, the risk is a combination of impact, likelihood, threats, vulnerabilities, and entity or assets (an asset is anything of value to an organization). Risk is usually measured as the amount of damage an asset would suffer in an adverse situation. Even though the risk is also an opportunity, as seen earlier in this chapter, we are going to examine risk more from the negative side throughout the rest of this chapter.

Risk management is based on the three elements of risk assessment, risk response, and risk monitoring. However, before we can even begin to assess risk, it is necessary to identify the assets that need to be protected and then determine the value of those assets to the organization. In the end, we must not spend more money to protect an asset than that asset is worth. This requires risk response to be based on the implementation of cost-effective controls.

Asset Valuation

The value of an asset is dependent on several factors - quantitative and qualitative values, and the criticality and/or sensitivity of the asset to the organization.

Determining Asset Value

What is an asset or entity worth? This is often quite a complicated calculation. The value of an asset is related to the cost of purchasing an asset, the importance of the asset to the business, and any regulatory issues. Price is often based on the value of the initial impact - but also on the ripple effect as the initial impact spreads to other systems, other departments, or increases over time. (the rise in incidence over time is part of a related discipline to be examined later known as Business Impact Analysis (BIA)).

Other factors affecting the calculation of the value of an asset include financial penalties for non-compliance with legislation, penalties for failure to meet service level agreements, the value of the asset (data or knowledge) to a competitor, the cost of reconstruction of the data or system, and impact on customer confidence, reputation or employee morale.

The reason to determine asset value is to ensure that the selection of controls is appropriate. An organization should not spend more to protect an asset than it is worth, but it should not ignore a risk that could have been mitigated at a reasonable cost.

Information Classification

Information classification is a crucial component in determining asset value. This is evidenced by the requirement in most privacy regulations to declare an information owner that must be responsible for the classification and protection of information. The purpose of information classification is to ensure that information receives an appropriate level of security. No organization wants to waste money and resources protecting information that does not require protection, or no longer requires protection. Nor does an organization want to face the liability and responsibility for not having protected information that should have been preserved.

Information protection is about setting in place the procedures, policies, and tools necessary to protect information at all points in the information lifecycle - from when it is first received throughout its various processes, storage, communications, and finally, its deletion. Information should be protected consistently and effectively from both internal and external misuse. The information should be protected at all times and in all locations. This is why the role of the information owner is so important. Information that comes into an organization may be stored or processed on several different systems, and those systems may all have different owners. The responsibility of the information owner is to set out the rules for the protection of the information that must be followed by all system owners regardless of what department the system owners are in. The information must also be protected in transit between systems or between the system and the client. The importance of enforcing consistent rules for protection is seen in regulations. Even an incident where an employee accesses information that is not required to perform their job function is a security breach. This is where the principles of "least privilege" and "need to know" apply most vigorously.

There are two main factors in classifying information - sensitivity, and criticality. Sensitivity refers to the issues of confidentiality and integrity. How sensitive is the information to disclosure (confidentiality) or modification (integrity)? Criticality is linked to availability. What effect would the loss of the data have on the organization? What impact would a delay in promptly having the correct information have on decision making or mission success?

The more sensitive or critical information is, the higher the level of protection that must be provided for it.

The classification of the information will often be based on the impact (consequence) of a breach of the information, and the frequency of an attack to determine the correct classification of the data. These are generally calculated using qualitative values such as Low, Moderate, or High[1].
The organization will usually handle many different types of information, and the protection required will vary according to the information type. The classification of the data is done first by looking at the various elements (types) of information the

[1] For an example of this see NIST SP800-60 http://csrc.nist.gov

organization handles, including items such as personally identifiable information, trade secrets or intellectual property, financial data. Then looking at each of the confidentiality, integrity, and availability factors separately by answering the following questions, "If there was a breach of confidentiality of this type of information we handle, would the impact on the business be low, moderate or high?"
"What would the impact on the business be if there was a breach of the integrity of this type of information?" And, finally, "What would the impact on the business be if this type of information was not available?"

Low would represent a limited level of impact - some cost, but the business would still be able to meet its core goals.
Moderate would be a more severe level of impact - higher cost and perhaps injury to a person, and a degraded level of service.
High would be a severe or catastrophic level of impact - loss of life or severe injury, high cost, or inability to meet core mission goals.

Once the impact has been calculated for each type of information the organization handles, the organization will group the data into categories and label the information accordingly. This effort of information classification will determine the controls necessary to protect each information classification or division. The rating of the information type will usually be based on the highest of the three levels of impact that were determined earlier. In other words, an information type that has an effect of the Confidentiality (moderate), Integrity (low), and Availability (Low) would be classified as Moderate since that was the highest of the three factors.

Most organizations will set out several categories for information classification, using, for example, terms like business private, confidential, proprietary, etc. It is essential to ensure that a suitable number of rankings are chosen. Too many could result in confusion between the difference in one or another. Too few and information that should be protected at different levels are grouped into the same category.

Each category of protection should have clear labeling and handling procedures. Every person that accesses information must know how to handle the data according to the policies and procedures. This requirement includes how the information can be shared, must be shredded, must be locked up, etc.

The information owner is responsible for ensuring that the procedures are being followed and that the information is being protected on all systems and at all times. This means working with system owners and departments to ensure that the data is being protected. This includes while it is on another network or even shared with business partners or outsourced service suppliers. The original information owner is responsible for the information when shared with another service provider or other organization unless that service provider explicitly and legally accepts responsibility for the info.

At some point in time, even protected information may be relegated to a lower level of classification or declassified altogether. There should be procedures in place to review the classification levels periodically. When classified information is no longer needed, it must be destroyed in a secure manner - shredding, physical destruction of magnetic media, etc.

Information versus Information Systems

All information must be classified to protect it adequately. However, once the data is categorized, it is also vital to categorize the information system that is used to display, process, store, or transmit the data. An information system can never be classified at a lower level than the information it contains. In some cases, the system may actually need to be at a higher level of classification since the information on the system may be subject to aggregation. Aggregation occurs when a user with access to the system may be able to combine the information on the network to gain knowledge about the information that is protected at a higher level than the individual pieces of information.

Summary of Information Classification

The classification of each type of information is based on the factors of confidentiality, integrity, and availability.
The information must have an owner that is responsible for determining how each information type must be protected and ensuring that the data is protected at all times and on all systems.

Each type of protected information must be labeled clearly electronically and/or physically to ensure it is handled appropriately.
There should be a process for declassifying information that no longer needs the same level of protection as it did previously.
The classification of an information system must be at least as high as the classification of the information on the network.

Now that the information has been classified, the risk assessment can begin. The risk assessment will need to determine asset value - which in many cases is dependent on the information classification.

Risk Assessment

Risk assessment is the evaluation and analysis of the consequence of risk and probability that an adverse event may occur, and, if so, how much damage (impact) that adverse event would cause. The risk assessment process will identify the risk to the organization, estimate the level of risk, allow risk to be prioritized. Which risk should be addressed before other threats, and justify some of the expense that will be associated with the response to or treatment (i.e., mitigation or reduction) of risk.

The output from a risk assessment is provided in a report describing the risk and listing recommendations on how risk should be managed. This also means whether the identified risk should be mitigated, avoided, accepted, or transferred.

Risk Analysis versus Risk Assessment

Some reference materials have a distinction between Risk Analysis and Risk Assessment; others do not. As we can see, ISACA does not make a significant distinction between the two terms - risk assessment or analysis are based on consequence and likelihood or probability.

ISACA defines risk assessment as A process used to identify and evaluate risk and its potential effects.

Scope Notes: Includes assessing the critical functions necessary for an enterprise to continue operations, considering the controls in place, and evaluating the cost for such restrictions. Risk analysis often involves an evaluation of the probabilities of a particular event.[2]

ISACA defines risk analysis as:
1. A process by which the frequency and magnitude of IT risk scenarios are estimated.

2. The initial steps of risk management: analyzing the value of assets to the business, identifying threats to those assets and evaluating how vulnerable each asset is to those threats

The ISO/IEC27005 considers risk assessment to include the phases of Risk Identification, Risk Estimation, and Risk Evaluation. It considers Risk Analysis to be the subset of Risk Assessment that only consists of the Risk Identification and Risk Estimation phases.

The NIST SP800-30 states that the two terms of assessment and analysis are synonymous. We will not make a distinction between risk analysis and risk assessment in this book.

What is Risk Assessment?

Risk assessment is the first step in protecting assets from threats. Risk assessment is a systematic process of identifying threats, exposing vulnerabilities, and rating the impact of an adverse event, no matter how it could happen - intentionally,

[2] ISACA Glossary www.isaca.org

accidentally, or circumstantially. Risk assessment is usually measured using either a quantitative or qualitative methodology, although most effective risk assessment programs will use a combination of both methods.

Quantitative Risk Assessment

Quantitative risk assessment is based on numbers - quantity. It attempts to place a numerical value (usually measured in financial terms, money) on the level of risk that the organization faces. It should be remembered that an organization faces many types of risk. Therefore will have many different risk assessment calculations depending on the impact on a system, department, or business process being assessed.

Qualitative Risk Assessment

Qualitative risk assessment is based on non-numerical categories or ranges of values. For example, the risk may be assessed using rankings of high, moderate, or low.

Identifying the Entity/Asset

Risk is an art and a science - but like any other project, it starts with a definition of scope - even a painter needs to know the size of the canvas! Performing a risk assessment starts with carefully defining the boundaries of the evaluation. Will this risk assessment be based on a system? On a product or service? On a geographical location? In a department? What is within the boundaries of the evaluation - what types of users, hardware, software, tools, processes, data, facilities, networks, or legislation? What is outside the scope, and what dependencies may exist between the area in range and the items outside of range? Can assumptions be made regarding issues outside the scope of this effort - can we just assume that the power requirements, for example, are being assessed in another risk assessment?

The assessor must understand the mission and goals of the area being assessed and determine how critical each asset is to the interests of the organization. This will aid in determining the asset value.

Threats

A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), corporate assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.[3]

The world is full of threats. Many are accidental - the accidental deletion of a field by a user or a simple mistake that interrupts operations. Many are intentional - ranging from script kiddies (inexperienced persons executing a low-level attack on a system) to criminal gangs and APTs. Many threats are based on natural events - earthquake, flood, tornado, or simply caused by equipment failure. The risk assessor must consider all relevant threats (threats that do not apply should not be considered). The likelihood of the threat must also be considered, but that can be done as a separate activity once all the risks have been

[3] NIST SP800-30 Rev 1 www.csrc.nist.gov

identified. Several documents list many of the dangers to review, including ISO/IEC27005 and NIST SP800-30 Rev1.

Threats are usually factors beyond the control of the organization. No policy will ever remove the threat of insider attack, nor will protection eliminate the risk of a tornado.

Vulnerabilities

A vulnerability is a weakness in a system or control that could be exploited by a threat. This may be an unpatched system, an untrained user, aging equipment, a building in a flood plain, or a control that is not being monitored and operated correctly. The risk assessor must consider the vulnerabilities since an asset with more significant weaknesses will be more likely to be exploited or suffer more damage than a properly defended asset.

Whereas threats are usually outside of the control of the organization, most vulnerabilities are within the power of the organization. It is through the recognition of weaknesses that an organization can select appropriate solutions and risk mitigation solutions.

Likelihood

The likelihood is the probability that an adverse event will occur or that a threat will exploit a vulnerability. The possibility is a complicated calculation or estimation to make since it is very subjective and unpredictable. Probability plays on the law of averages - how often have things happened in the past? But that may not be an accurate predictor for the future. A future event may never arise or may happen more often than it has in the past. The risk assessor may rely on statistical data or examples from other industries to make likelihood determinations.

An essential factor in vulnerability assessment is the capability of the adversary. An adversary that is motivated and skillful is a much higher risk than a dispassionate hacker that is just wandering around seeking targets of opportunity.

Insurance companies rely on empirical data and historical trends to predict risk. Still, in the information security world, the threat environment is under continuous change, and the effectiveness of controls can be hard to assess. We have seen companies that had no data breaches for years suddenly fall victim to many violations in a few days. We have seen products that were once thought to secure.

Impact

Just like likelihood, determining the level of impact an event would have is a very challenging and elusive calculation. It is tough to know how much damage an event would cause if it were to happen, and most often, the estimates are very inaccurate. Organizations frequently underestimate the loss - not considering the damage to reputation, customer confidence, or employee morale correctly. The forecast of impact must consider the maturity of the business and its ability to respond quickly and effectively to an incident, but also must consider factors such as the health of the relationship with customers and regulators, financial depth, politics, labor troubles and extent of vulnerabilities.

The level of impact may also depend on the extent and effectiveness of controls in place to prevent or contain an incident.

Risk Level

The risk level is a combination of all the above factors - asset value, threat, vulnerability, likelihood, and impact. The risk may be measured either quantitatively or qualitatively - or as a hybrid of both. As we can see, the critical factors in risk assessment are to be able to assess the threat and vulnerability environment accurately. We use professional judgment to evaluate the capabilities and motivation of the adversary, the strength of the controls, and the effectiveness of the security program.

Quantitative Risk Assessment

Quantitative risk assessment starts with the calculation of the impact of a single adverse event and then calculates the annual cost of risk based on the number of times that event may happen per year. Using a yearly basis provides a common denominator to compare various types of risk with each other. This is primarily since most budgets and risk management efforts are based on annual budgets.

Single Loss Expectancy (SLE)

The calculation of Single Loss Expectancy (SLE) is a part of a quantitative risk assessment. SLE is simply calculated as the Asset Value (AV) multiplied by the Exposure Factor (EF).

SLE = AV * EF

As seen earlier, the value of the asset is determined by calculating all costs related to the loss of, or compromise of, an asset. The exposure factor is the amount of damage experienced in asset value due to an attack.

This calculation provides the amount of loss an organization could and should expect from any one event. For example - if a building was flooded out or caught fire - what would the amount of damage be? In most cases, the building would only experience a partial amount of damage. Therefore the exposure factor would only be equal to a partial amount of the total asset value, not identical to the full cost of the asset. That is why the exposure factor is used as a percentage of the damage suffered.

It must be remembered, however, that the cost of an incident is much more than just the direct, initial price. The value includes the impact on productivity, the loss in customer confidence or reputation, and the costs of litigation or contractual violations. In some cases, historical records, events that have happened to other organizations, or other sources may aid in determining the value of a single incident.

There are many different types of adverse events that could happen. Therefore, the calculation of SLE may need to be done many times for various activities, various departments, different systems, and different times of the year.

Annualized Rate of Occurrence (ARO)

One of the most challenging calculations for a quantitative risk assessment is the frequency or likelihood of an unwanted event occurring. This is especially difficult when trying to predict a development that is related to new technology, or that has not happened previously. In this case, historical data is not available, and determining the probability of a risk event is based primarily on guesswork.

Since events will happen at various intervals, using a common denominator of an annual measure is useful so that a comparison can be made. Since most security budgets are also calculated yearly, the use of a yearly risk calculation is better suited to supporting budget calculations.

The formula for ARO is simply:
ARO = Incidents / Year

Annualized Loss Expectancy (ALE)

ALE is the combination of Single Loss Expectancy (SLE) and Annualized Rate of Occurrence (ARO).

ALE = SLE * ARO

Therefore if an event that would cost $1,000,000 would happen once in ten years the formula would be:

ALE = 1,000,000 * 1/10
ALE = $100,000

The purpose of this calculation is to provide justification for risk mitigation activities since it would never be wise to spend more to protect an asset than it is worth. To focus on the areas of most significant risk before addressing less critical risk factors. Since most organizational budgets are based on an annual cycle, using the ALE aligns the risk value with the budget cycle.

Problems with Quantitative Risk Assessment

The problem with a quantitative risk assessment approach is the lack of accurate data that can be used in the calculations. Even where there is excellent historical data, factors may change that significantly alter the trustworthiness of the estimates. It also takes a lot of time and effort to complete an accurate (or at least as precise as possible) quantitative risk assessment. Risk assessment requires the input of many experts, interrupts business operations, and may create some resentment about the value of the risk assessment, especially concerning the amount of work and time required.

The results of a quantitative risk assessment will be a report that lists the risks and indicates their relative cost. This allows for the prioritization of risk and the development of a risk response strategy that can be based on cost-benefit analysis.

Qualitative Risk Assessment

The foundation for qualitative risk assessment is the ranking of the level of risk for various risk scenarios. Instead of putting absolute (monetary) values on the cost and likelihood of an event as seen earlier in quantitative risk assessment, qualitative risk assessment uses a range of benefits to measure impact and probability.

One example of this is the ISO27005 process, which is primarily a qualitative approach using the range of values for both impact and likelihood of Very Low, Low, Medium, High, and Very High. Other methods, such as the NIST SP 800-30, uses three levels of ranking.

Figure 8

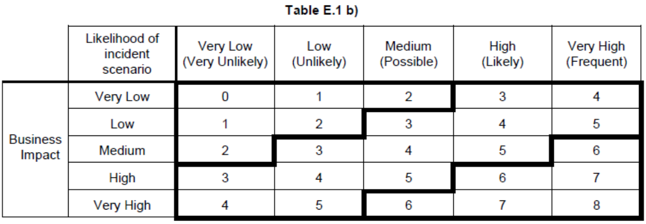


Table E.1 b)

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

ISO 27005 Appendix

Using a table of values such as this may allow a little more understanding and acceptance of the value of the risk assessment above and beyond the declaration of an absolute value for risk, as seen with a quantitative approach.

A qualitative risk assessment approach often relies on the input of many individuals representing all the lines of business and viewpoints. The value of this is that it often highlights the dependencies and relationships between departments.

Gathering Information

Information used in a risk assessment can be gathered in several ways. The most common method is probably through surveys. Surveys can be cheap, easy, and inaccurate. The value of the information provided in the survey is subject to the quality of the questions asked and the motivation of the respondent to reply. A restaurant may ask for feedback, but if the patrons know that it is not likely to be heeded, they may not care what they say and take the time to answer accurately. The responses may be based more on what the respondent thinks the survey wants to hear, and the person initiating the survey may well ignore responses that do not fit into their desired model.

The risk assessment is only as good as the information it is based on - so care must be taken to ensure that accurate and complete information has been provided. As will be seen later in this book, the reason most projects fail is that the requirements were not properly documented or understood by all the team members.

Other methods of gathering data include interviews, facilitated workshops, observation, audit reports, reports of previous incidents, penetration tests, and the Delphi method.

The Delphi method is an excellent way to gather accurate data, especially in an environment where strong personalities exist and may otherwise attempt to influence the data gathering process. The Delphi method is based on anonymous input and feedback from a wide range of participants representing all areas of the organization and each level of management and user. To perform a Delphi-based risk assessment, the facilitator will send a question to all the participants that they must answer anonymously and confidentially - preferably without discussing their answer with any other participant. The responses are then collected and redistributed to everyone so that they can see all of the responses. The participants are then asked to rank the top priorities amongst all the responses. Everyone gets to contribute - work together towards a consensus and plan of action. This may overcome the disadvantage of a facilitated workshop where only select people may be invited and where one influential person can push their opinion over the entire group.

The result of a qualitative risk assessment is a ranking of the most serious risk to the organization. It indicates the priorities, the risk that must be addressed immediately as compared to the risk that can be either addressed over a longer period as resources and opportunities are available and which risk may just be acknowledged and accepted.

Problems with Qualitative Risk Assessment

The problem with qualitative risk assessment is that it does not indicate the monetary cost of risk and yet the selection of controls must consider the cost of the control versus the benefit of the control in reducing the monetary value of the risk. This makes it hard to convince senior management to spend the money necessary to deal with the risk without being able to show any financial data or concrete results. As with all risk assessments, it is partially guesswork. An event may not happen for years and then may happen several times in one month. It is nearly impossible to predict the true cost of an incident, especially in a world of social media and unpredictable levels of media attention. As is often said - if you have an incident, hope that it is not on a slow news day where you are the only story in town!

Hybrid Risk Assessment

Neither the Quantitative nor Qualitative risk assessment approach is perfect or ideal. Therefore, the two are used together in a hybrid model to gain a better appreciation for the risk assessment from both a monetary and non-monetary perspective.

Other approaches that may be used include models such as the Failure Modes and Effects (FMEA) model and the Fault Tree Analysis (FTA) model.

Risk Assessment Report

The results of the risk assessment - whether done through a quantitative or qualitative approach, or both, should be compiled into a risk assessment report (RAR). This report will outline to management what the risk is, the severity of the risk and priorities for risk response, and recommendations on how to deal with the risk in an effective manner. This report is provided to management to inform them of the risk and allow them to initiate the response process.

Risk Response

The final step of the risk assessment phase was the creation of a risk assessment report (RAR), which is the input to the next phase in risk management - the risk response phase. In this phase, management will make decisions on how to address the identified risk and how to schedule risk mitigation activities. There are four primary ways to respond to risk - to accept the risk, to avoid the risk, to mitigate the risk, or to transfer the risk.

Risk Acceptance

The first step is to know the risk appetite of the senior management team. This will determine which risk can merely be acknowledged and accepted, and which risk must be mitigated or transferred. The level of risk acceptance is also dependent on regulations and compliance mandates that the organization must adhere to. When considering cost-benefit analysis, it can easily be understood that management is not interested in spending more money to address a risk than the asset itself is worth. Management is also reluctant to spend more on control than the benefit obtained by that control. Therefore, a certain amount of risk will be accepted as a cost or risk of doing business.

The critical factor in accepting risk is the accuracy of the risk assessment level. An organization may accept a specific risk under the impression that the level of risk is much less than it actually is. This emphasizes the requirement for the risk assessor to be thorough, complete, accurate, and honest in their assessment. Note that only senior management has the authority to accept risk on behalf of the organization.

Risk Mitigation (Reduction)

When the level of risk is unacceptably high, then the organization may choose to implement some form of control to decrease the risk level. Each control should reduce the risk significantly while still preserving a favorable cost/benefit ratio.

In other words, the cost of the control should be significantly less than the value (benefit) provided by the control. A control cannot remove all risks - there will still be a remaining level of risk to the organization. This is the residual risk. The purpose of the risk mitigation effort should be to reduce the residual risk to a level that is equal to or less than the acceptable risk. Please note that residual risk is not the same term as risk acceptance. Residual risk is the total risk of less control effectiveness - the risk that remains after implementing a control. In contrast, risk acceptance is the threshold or level of risk that senior management is willing to accept. The goal of a risk mitigation effort is to ensure that the residual risk is less than or no more than the risk acceptance level set by management.

Most risk controls address vulnerability and will reduce either the likelihood or impact of an adverse incident. A fire extinguisher, for example, does not reduce the likelihood of a fire - it only contains the amount of damage a fire may cause. A no-smoking policy in an area where flammable gases are present reduces the likelihood of fire but does not reduce the impact if there were to be a fire. It is practically impossible to eliminate the threats - those will continue to exist. All the analysts can hope for is to reduce the ability of that threat to pose an unacceptable level of risk to the organization.

As seen earlier in the chapter, a control may be administrative (managerial), technical or logical, or physical. Good control is one that reduces risk but does not cause an undue impact on the operations of the organization.

Many controls will be implemented in layers of defense so that one control augments or supports the other controls and so that a failure of one control is covered by subsequent controls.

Cost of Controls

Since the choice of control is based on cost versus benefit, it is important to understand the true cost of the control. The cost of control is based on many factors, ranging from the initial purchase and implementation cost, licensing costs, maintenance costs, impact on productivity, impact on insurance premiums (which may be either a benefit or a cost), and impact on resources. Often, risk will be mitigated through a series of controls that work together in a defense-in-depth approach. However, the "Law of Diminishing Returns" applies here. The more money spent on implementing controls, the less value each successive control will provide until it can be said that a lot of money could be spent for almost no tangible benefit.

Risk Transference

In many cases, an organization may choose to reduce their level of risk through the purchase of insurance or some other form of risk transference. This shares the cost with another organization and can protect the organization from some of the financial liability associated with an adverse event.

Risk Avoidance

There are risk-laden situations where there is no suitable way to address the risk or reduce the level of risk to an acceptable level. In this case, the organization may choose to avoid the risk altogether and cease the activity that is associated with the risk. This may mean stopping operations in a region of the world, ceasing the manufacturing of an outdated product, or shutting down an older system.

Implementing Risk Response

Once the risk assessment report has been submitted, and the organization has a chance to review the recommendations of the risk assessors, the next step is to put in place a plan to respond to the risk. The risk assessment identifies the risk and suggests the priorities for risk mitigation. However, it is up to management to determine the gap between current levels of risk and risk acceptance levels. The risk assessor may recommend controls. Still, in the end, it is up to the senior management team to determine whether to accept the recommendation, implement even more stringent controls than were recommended, or accept a higher level of risk than was recommended. This is based on the risk culture of the organization and the risk appetite of the senior management team.

Once the mitigation strategy (accept, transfer, avoid or reduce the risk) has been chosen, the next step is to put in place a plan to implement that strategy. This is where the organization must consider the risk priorities, available time and resources, and cost. The priorities for the risk response strategy may be based on legal requirements and compliance. The severity of the risk, the availability of a solution, and perhaps the implementation of some quick wins can show progress. Like any security program, the risk response plan should be based on deliverables, milestones, and results. The program should report back to management on the status of the project and the effect on the risk profile of the organization.

Risk Monitoring

No control will work forever, no control is 100% effective, and no risk will remain the same indefinitely. Therefore the final phase of risk management is the ongoing monitoring of risk. Regular risk assessments, reporting to management, scheduling of implementation of new risk mitigation efforts, and evaluation of the effectiveness of the controls are all part of the risk monitoring effort.

The frequency of risk assessments and reporting are often mandated by law (FISMA in the USA requires annual reporting to Congress), policy, or industry standards (PCI-DSS requires a penetration test every quarter.) Many factors can affect the risk profile of the organization, including emerging threats, newly discovered vulnerabilities, political changes, supply chain failures, natural events, changing markets, and aging of equipment.

All of these should trigger a review of the risk and a report on any changes to the risk levels facing the organization. Other factors that affect risk can be significant changes to an application, hardware upgrades, or changes in the user community. For this reason, risk monitoring must be integrated into the change management process. To determine if the change will affect the overall risk, the effectiveness of controls, or possibly of violating regulatory requirements.

The measuring of control effectiveness is often based on the development of a control baseline. The control baseline is the desired minimum state for the security program, and all parts of the organization should meet that baseline. Areas of non-compliance should be identified to management to enable mitigation and address the risk gap.

The ways that controls can be monitored can be described as IDOT (Interview, Document, Observe, and Test.) The risk assessor should interview the parties responsible for the risk to ensure that they know the procedures, are familiar with their responsibilities, and know how to report any non-compliance.

The documentation should be up to date and current - reflecting current procedures in use. Observing the behavior of the system is important to ensure that the controls are operating correctly and that the administrators of the controls are doing their function correctly (there is often a disparity between knowing what should be done and doing it). Testing is the actual testing of the control to ensure it is working correctly and that the control is, in fact, mitigating the risk. It must be remembered that the purpose of a control is to mitigate risk, not just to be a functioning control!

Risk monitoring is an ongoing process that must be integrated into all business functions and be a part of all new initiatives, business activities, and strategic investments. Major changes to an organization's business processes such as mergers, acquisitions, new product lines, new business models (online, etc.) should all include risk evaluation in the planning and deployment process. As can be seen here, risk monitoring overlaps with and leads back into the process of risk assessment in the never-ending cycle of risk management. The use of standard metrics to assess risk is also important so that changes in risk and potentially harmful trends can be identified.

Vulnerability Assessments and Penetration Tests

Risk monitoring includes regular vulnerability assessments and penetration tests that can be conducted either internally or externally.

A vulnerability assessment is a valuable tool to identify any gaps or misconfigurations in the security profile of the organization. A vulnerability assessment is like walking around a building, ensuring that all doors, windows, and other points of entry (loading docks, etc.) are locked and secure. The vulnerability assessment of an information system is a methodical review of security to ensure that the systems are hardened and that there are no unnecessary open ports or services available that could be used as an attack vector by an adversary or misused by an internal employee.

A vulnerability assessment often results in a lot of 'noise' or alerts about vulnerabilities that are not serious. This requires the expertise of a security expert to analyze the data from the vulnerability assessment and determine which results are significant and which results can be ignored.

A vulnerability assessment is often a thorough review of an entire system or facility, and it is intended that the assessment will provide a good, complete review of all security controls. This can include both technical and non-technical controls. For example, a review of a firewall would often include the review of the configuration (technical), but also a review of the change control process for managing the configuration. Through such a vulnerability assessment, management can gain a solid report on the strength and effectiveness of the risk management program. Many open-source and commercial tools can be used to perform a vulnerability assessment. Several websites list known vulnerabilities with typical applications, operating systems, and utilities.

The problem with a vulnerability assessment can be the number of false positives or "noise" that it generates. This can make it difficult to determine the actual severity of the problems. Therefore, the next step is to conduct a penetration test.

A penetration test is a targeted attempt to "break into" a system or application (or in a physical check to break into a building). The penetration tester, using the results of a vulnerability assessment, will select a potential vulnerability and try to exploit that vulnerability. If the penetration tester can break-in, then the weakness is real and must be mitigated. If the examiner is unable to break in, then there is a good chance that the vulnerability is not severe and does not require mitigation.

A penetration tester often uses the same tools used by hackers to try to break into systems. This means that the results are quite real and do provide meaningful results. However, this also poses a risk to the organization since these tools can be hazardous to use and may result in system failure or compromise. Therefore it is of utmost importance that such tests are only conducted with management approval and through the use of a defined methodology and oversight.

The results of the penetration test will be provided to management for follow-up and review.

There are many useful tools that a risk manager can use when monitoring risk. These include free reports from anti-virus and security companies, including (but not limited to) Microsoft, SANS, Symantec, F-Secure, McAfee, and Trend Micro. Other data, such as the Verizon Data Breach Investigations report, are issued annually. They provide a review of risk and exposure factors and may assist in developing and presenting a risk management solution to management. Other sources of information on incidents and risks come from government sources such as local or national CIRTs (Computer Incident Response Teams) and not-for-profit organizations.

Reporting on Risk

There are several ways that risk should be reported to the organization. Senior management should receive scheduled reports on the current risk levels of the organization and the status of risk mitigation efforts. These reports are often non-technical and may indicate whether the organization is compliant with international standards or best practices. Quite often, such statements are more of a summary with key points than a detailed description of the risk program and assessments. Penetration tests and vulnerability assessments are usually more technical and detailed. These reports are provided to IT staff and management with details of the findings so that necessary changes to control configuration and placement can be made. Audit reports are a standard method of communicating risk and control effectiveness to management. Audit reports usually contain two sections - an executive summary that provides a high-level overview of the audit and a detailed audit report that includes the details of the findings and recommendations of the auditor.

Summary of the Risk Chapter

Risk is an essential part of business today - whether that business is government, military, commercial enterprise, or even a not-for-profit endeavor. The management of that risk is one of the primary responsibilities of the security professional. Risk management starts with the careful, systematic assessment of risk to the assets of the organization - based on the value of assets, the types of threats, and the vulnerabilities associated with operations.

Risk management then continues to determine the appropriate response that needs to be in place to address the identified risk through the selection of controls, risk acceptance, avoidance, or transference. Risk is not static and therefore requires careful monitoring.

CHAPTER THREE: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT

Security Program Development

The development of a security program is the implementation of the security strategy. As seen earlier, the security strategy is just an extension of the overall business strategy of the organization. The business needs to see that the implementation of security is aligned and integrated into the mission and goals of the company. Security is implemented for the sake of the company - to help the company meet its purpose - not just for the use of security and to "be secure."

The security strategy must also be aligned with the other policies and operating procedures of the business, including human resources, finance, operations, legal, and lines of business.

As businesses evolve and move into new lines of business - perhaps outsourcing, cloud, and mobile computing, so also must the security program adjust and support those developments. Security must not be an anchor that continuously holds the business back and prevents growth. Just as the company seeks to remain competitive, so also the security department must lead the way by developing standards and procedures that will enable the use of modern technology.

Requirements

Many information technology projects fail to deliver what the business really needed or expected. Instead, they provide a product not correctly aligned with business requirements, and that may be difficult for the users to use. This also happens with security, projects that should have strengthened the organization. This makes it more resilient, more responsive, or more robust. When we examine the reason that so many projects fail, we hear a common theme - "the requirements were incorrect," or "the requirements changed."

Of course, the requirements changed! A business faces two problems when it comes to needs: first of all, they do not really know how to describe their needs. Secondly, by the time the project is finished, the business has evolved into a new operational world!

Therefore, we must understand the business. We need to see security from the perspective of the company and examine their processes and their requirements. Once we know the organization, only then are we able to develop a security solution that is ideal for the company. The key to remember is that security is dependent on the company, not the other way around.

Gathering the security requirements is often as much about education as it is listening. The sources of our needs - the people in the business - usually do not know what security really is or what we are trying to do. Their perception may be that security is to implement strong passwords - they do not consider, perhaps, the needs for availability, error handling, redundancy, access controls, and resistance to attacks. The business, as we would expect, will usually describe their requirements from the perspective of how the process should work, and how to handle the normal errors that occur. This focus on function is perfect for designing a system that will work under normal conditions but is incomplete. Their approach is focused only on how to misuse the system or allow it to be used for their purposes.

An example of this is the 'ping' (ICMP) service that administrators use to test network connectivity. The Ping was a small 32-byte packet that would initiate a response from a remote device. This would prove that two devices could communicate over a network. Over the years, we have seen how hackers misused the ping packet in ways that were totally unrelated to its correct function.

They created the "SMURF" attack to flood a device with responses, a malformed ping into a large packet that could disable a remote device in the 'ping of death' attack. Attackers use it for mapping a network - all purposes which were unintended uses and could interrupt system operations.

Since ping had been designed for a simple function, it had no defenses to protect against its misuse. This explains why we must consider the threat vectors and misuse cases of a system when building it. Every system built today should be built with the expectation that it will be attacked and, therefore, be built with the ability to withstand an attack and continue to function correctly. One of the tools that can be used to gather requirements and assist in the alignment of security with business needs is SABSA (*www.sabsa.org*). SABSA is an open-source framework that guides a team through the requirements definition process. It takes a top-down approach to understand the context and high-level strategy of the business and then working down through the layers of business units (concept), information systems, data, and individual components. What a top-down approach does is to ensure that the more detailed levels of the system are designed and developed based on the larger picture of the overall business requirements and systems integration. Other models that use this same approach are Zachman (*www.zachman.com*), TOGAF (*www.opengroup.org*), and ITIL (*www.itil.org*).

The implementation of the information security strategy is founded on the use of people, processes, and technology all working together. It can be said that an information security program is having the "right" people (personnel with the necessary skills and training) using the "right" products (products/technology that is being used correctly) in the "right" way (with correct procedures and operational controls).

A misconfigured firewall, or a lack of change control procedures, or an untrained administrator can all lead to a serious security breach. Security is a fabric of several threads that must be woven together - every thread is important, and any break in the thread can affect the integrity and strength of the entire fabric.

A security system is based on a foundation of policy. The policy directs the implementation of security and is the authority behind procedures, standards, and baselines. Procedures are the implementation of policy into practical steps that result in consistent operations. Following a procedure, ensures that all users will be set up correctly in a manner that would identify any inconsistencies and alert management to potential risk. The use of standards allows the organization to leverage the benefits of using a standard product, which can result in savings in training, spare parts, acquisition, and incident handling.

The use of baselines ensures that systems are configured consistently. This ensures that all systems meet, at a minimum at least, a defined level of security. These are all valuable tools to take the intent and objectives of policy and develop them into a practical and auditable security framework.

Guidelines are often helpful to assist users in following the standards and procedures. While guidelines themselves are recommendations (policy, procedures, standards, and baselines are mandatory), a guideline is an excellent way to help users understand how to meet requirements. Guidelines, for example, may describe how to create a good password, or other suitable security practices and behaviors.

The security program must be documented, and the documents keep up to date, to ensure that everyone is familiar with their responsibilities and to allow auditors the opportunity to review compliance with the security program. The documents should outline the correct procedures and requirements and detail the steps necessary to be compliant with the security controls.

Controls are to be based on risk, and therefore, there should be a clear alignment between the control and the risk that the control is mitigating. Education on the purpose of control and the risk that it is intended to address may also encourage compliance with the control and greater acceptance of the control.

Important Procedures

Control Monitoring and Reporting

With careful design and implementation, an organization may deploy a good security program, but the risk is that, over time, the security controls may become ineffective. Changes may happen in networks or applications that bypass the controls, the users may stop following procedures correctly, or administrators may take shortcuts. This is why it is important to monitor security controls regularly. Monitoring the controls, including tracking KPIs and

KRIs, can alert management to trends or changes in risk that may be a sign of a potential breach. There are many ways to review controls, including log reviews, alarms, incident reports, and user feedback.

Reports that show comparable results and can indicate trends inactivity should be provided to management. The reports, however, should be based on metrics that are good indicators of system security. There may be many points at which a system is being monitored, but not all logs need to be reviewed.

The reports should focus on areas of most importance. All logs should be protected and retained so that they are available for later review and investigation. Writing the logs onto a separate media that would prevent the deletion or modification of log entries may also be desirable. The length of time that logs should be retained is dependent on legal requirements, business needs, and the value of the information in the logs. Some logs may need to be retained for years to be compliant with laws and regulations; other logs may be deleted or overwritten in a matter of days.

Change Control

A time of change is a time of risk. A change may interrupt business processes, bypass controls, lead to project overruns, and scope creeps or render business continuity plans ineffective. Therefore, the organization should have a clearly defined and followed change management process. This will ensure that all changes are formally requested and documented, reviewed for their impact on the business and security, and tested and approved before implementation.

Change control procedures should be used for all changes to projects, networks, applications, configurations, and user permissions. The tracking of changes ensures that changes are completed correctly, that no unauthorized changes have been made, and that all changes have been tested before deployment.

The change management process will also coordinate the scheduling of changes to ensure that a change is done at the time most suited for the business. Changes should not be done at operationally critical times unless an emergency change is needed.

The final step in the change control process is notifying management of the completion of the change.
A part of the change control process should be the notification of the potential change to the business continuity and disaster recovery teams. This ensures the BCP and DR plans can be updated. It also ensures that the correct files, applications, and configurations are being backed up.

Backups

Equipment failure is to be expected, and hardware has a Mean Time Between Failure (MTBF) rating that indicates the expected lifespan of the device. Organizations should have an asset tracking system that is tracking equipment and ensuring that the equipment is being maintained and replaced on a scheduled basis. Many organizations can find that they have previously undiscovered vulnerabilities since they are running equipment and systems that are well past their expected lifespan.

To be ready for equipment failure or the accidental deletion of files, it is important to have backups of all system files, configurations, transaction files, operating systems and applications, patches, and reports.

Backups need to be tested to ensure that they will work when needed. Keeping one set of backups offsite is a good idea to be prepared for the loss of the primary information processing facility. The traditional method of storing backups was on tape, but the tape is a rather slow process for data recovery.

Third-Party Relationships

Most organizations today use various third-party services to support their business operations. These can range from cloud providers to call centers and payroll service companies to offshore manufacturing.

These relationships pose a unique set of challenges to the security manager. So when the organization's data or intellectual property is being held offsite, the organization must ensure that its data is being protected according to laws, policies, and best practices.

The ownership of the data of the organization remains with the organization that received the data initially. This includes even if the data has been sent to another company. All contracts with third parties should address the ownership of, and responsibility for, protection of the data. The contract should address what jurisdiction will be used for any dispute.

When data is being sent offshore, the organization must verify that this is acceptable under data privacy laws. The laws of many countries restrict the movement of their citizens' data to an offshore location.

Cloud Computing

Over the past few years, a lot of organizations have moved to cloud computing as a model for data processing and storage. The use of a cloud-based service such as Software as a Service (SaaS) is an excellent way to support business requirements without the need to install and maintain applications on every desktop. Instead, all an employee needs to be able to access corporate data, and application functionality is a web connection and a browser.

The hosting company does all application patches, stores, and processes data, generates reports, and provides protection for the data. As with any outsourced service, the need to ensure that data is being protected is available when required, and can be retrieved in case of termination of the contract.

Other cloud-based services such as Storage on Demand, Infrastructure as a Service, Platform as a Service and email hosting are all popular since it removes the requirement for the outsourcing organization to manage, acquire and maintain their own IT infrastructure. The security professional must ensure that the network connections to the hosting company are secure and that the hosting company has backups and disaster recovery plans.

Mobile Computing

Many services provided by organizations today are moving onto mobile platforms such as online banking and email. These services are run using mobile applications and application program interfaces (APIs), often on top of legacy systems and more traditional information systems. This requires attention to the coding practices of the organization and the choice of APIs used. Using an insecure or older API may present an attack vector that could be used to launch a man-in-the-middle attack or highjack a user session.

The other concern is that most of these mobile applications are running on personal devices that may be infected or compromised without user knowledge.

BYOD

Organizations are embracing the concept of Bring Your Own Device (BYOD) or sometimes jokingly referred to as Bring Your Own Disaster! The BYOD approach makes a lot of sense from a business perspective. Everyone can use devices that they possess, including mobile phones, tablets, laptops - devices that they are comfortable with, and that may save the organization the cost of purchasing!

This does, however, pose some security concerns. What happens when the person leaves the company - especially involuntarily - is it possible to remove all organizational data from the device? What if the device is compromised, lost, or stolen? Is the confidential data on the device protected?

There are several solutions the security manager must consider, including first and foremost policy. It is also possible to declare which devices are allowed and which are not. A virtual machine that can be remotely wiped in case of loss can be set up on some devices. Some devices will also allow encryption and two-factor authentication for access.

As with all new technologies, the security manager must often understand that it may be impossible to stop the use of the new technology, but it is possible to put in place security controls to protect the use of the new technology as much as possible.

Cryptography and Digital Signatures

Cryptography is the art and science of protecting the confidentiality and integrity of data. Through the use of cryptography, it is possible to protect data when stored or transmitted, even when it is being transmitted over insecure mediums such as radio, satellite, and the internet.

The five main benefits of cryptography are:

1. Confidentiality - keeping sensitive data private
2. Integrity - maintaining the accuracy of data
3. Access Control - preventing access by unauthorized users
4. Non-repudiation - linking activity to a known entity (individual or process)
5. Authenticity - being able to ensure the identities of the source and destination entities - knowing who sent what and validating the destination

Not all of these benefits are available through all types of cryptography. Various types of cryptographic algorithms and implementations offer different services. The security professional needs to know which benefits are provided by which type of implementation.

The key definitions associated with cryptography are:

- Plaintext/cleartext - the message in its normal readable format.
- Ciphertext/cryptogram - the message in an unreadable format
- Encrypt/encipher.encode - the process of converting plaintext into ciphertext

- Decrypt/decipher/decode - the process of converting ciphertext into plaintext
- Algorithm - the mathematical process used in the encryption/decryption process
- Cryptosystem - the mechanism or device used for encryption/decryption. The algorithm is a part of the cryptosystem
- Initialization vector - a random value added to the initial step of the encryption process to ensure that even similar messages look different once encrypted.
- Substitution - replacing one value for another. For example, the Caesar cipher replaced each letter of the message with the letter three places further down the alphabet.
- Transposition - changing the position of the letters so that the letters in the ciphertext are not in the same order as the letters in the plaintext
- Work factor - the amount of time or effort (resources) needed to defeat a cryptosystem.

Symmetric Algorithms

Symmetric algorithms have been in use for thousands of years. Their main benefit is protecting the confidentiality of messages. The symmetric algorithm is one that uses the same key in the encryption process as it does in the decryption process. The two operations are really a mirror image of one another - therefore, the use of the term symmetric.

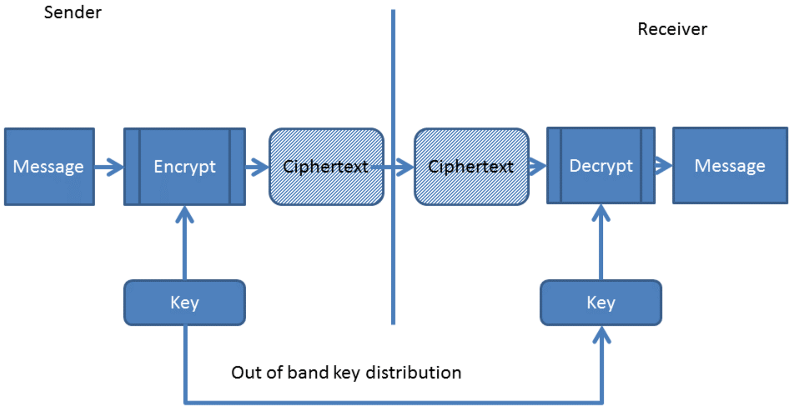


Fig 10 Symmetric Cryptography

Symmetric algorithms are fast, and most are free. Some of the common examples are AES, RC5 and RC6, MARS, Serpent, and Blowfish. These are all tested and proven products that can be used for data encryption for transmission and storage. The older algorithm of DES is no longer trusted. RC4 is a stream-based cipher used in wireless products that use WEP (no longer trusted) or WPA. WPA2 is based on the implementation of AES.

The weaknesses of symmetric algorithms are mostly related to key distribution and management. To use the symmetric algorithm, both the originator and receiver of the message must have the same key. This means that either person can read or alter the message, and no one can prove whom the last person to access the message was. This also means that every pair of people that want to communicate must have a separate key that only they use. This requires the storage and distribution of many keys.

Key distribution is also a challenge since there must be a secure way to share the symmetric key between the two parties without anyone else getting a copy. This means that the key cannot be sent in the same channel as the data but must rather be sent out of band or in some other distribution channel (courier, fax, phone).

Asymmetric Algorithms

Asymmetric Algorithms are a relatively recent development. In the 1970s, Diffie-Hellman developed a method of encryption based on two different keys. The two keys are mathematically related. One key is known as the private key; the other is known as the public key. It is not computationally feasible to learn the value of the private key even though a person knows the value of the public key. Therefore a person may freely and openly give their public to everyone without risking the compromise of their private key. Because asymmetric algorithms use a public and private key pair, they are commonly referred to as public-key algorithms.

The main use of most asymmetric algorithms is to support the implementation of symmetric key algorithms and for digital signatures, which will be examined later.

Diffie-Hellman was used to allow two parties that wanted to communicate over an untrusted network to establish a secret key that could be used for symmetric (fast) encryption. Therefore it is known as the key agreement protocol. This is used in some internet applications and in IPSEC.

Several rules can be used to remember how asymmetric algorithms work. Remembering these rules can make the understanding of asymmetric algorithms a lot easier.

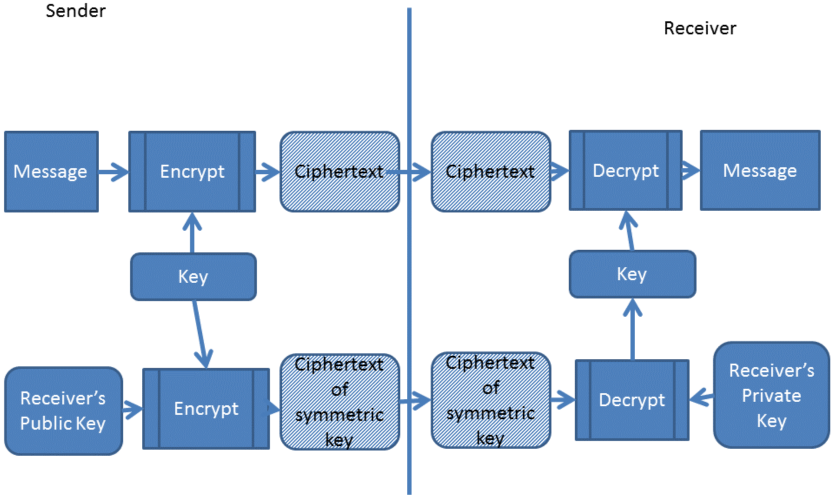
The first rule is essential - that is:
The keys in an asymmetric algorithm only work as a pair. When one key (one half of the key pair) is used to encrypt a message, the other half of the key pair is the ONLY key that will successfully decrypt the message.

Confidentiality

The use of other asymmetric algorithms has been to distribute the secret symmetric key between two parties that wish to communicate. This is in contrast to Diffie-Hellman that was used to negotiate the secret symmetric key.

This can be done as follows:

Fig 11 Using Asymmetric algorithms to Support Symmetric Cryptography



As can be seen from this diagram, Alice can choose a secret symmetric key that she wants to use to talk confidentially with Bob. She can securely send the symmetric key to Bob by encrypting the symmetric key with Bob's public key. Since it is encrypted with Bob's public key, Bob must open it with Bob's private key - and since he is the only person that would have his private key - the message (which in this case is a symmetric key) can only be accessed by Bob. Then when Alice sends a secret message to Bob that is encrypted with the symmetric key they just shared, Bob will have the symmetric key he needs to decrypt the secret message.

So rule number two for asymmetric algorithms is:

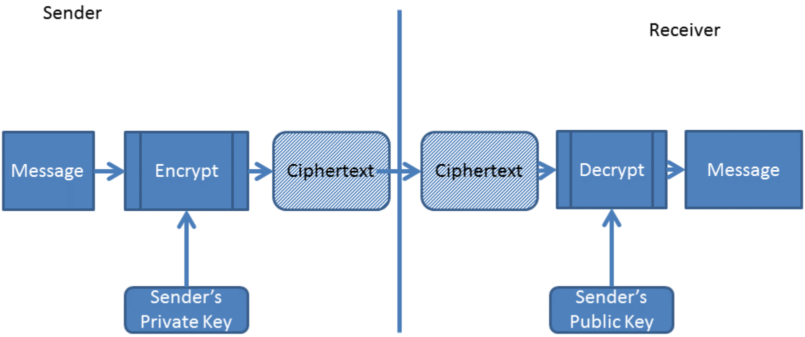
Encrypting a message with a public key provides confidentiality since only the holder of the private key that is linked to that public key can decrypt the message.

Proof of Origin

Another benefit of asymmetric algorithms is the ability to provide proof of origin.

This can be done, as shown below:

Fig 12 Proof of Origin Using Asymmetric Cryptography



As can be seen here, Alice has encrypted a message that she wants to send to Bob with her private key. This means that anyone with Alice's public key could open the message. Therefore the message is not confidential. However, since the message can be opened with Alice's public key, it must be known that the message was encrypted with Alice's private key. Since Alice would never share her private key with anyone, we know that this message must have come from Alice. Since the message Alice sent is not confidential - anyone with her public key could read the message - we refer to the operation of encrypting a message with a private key as 'signing' the message. Note this is not the same as a digital signature, which we will look at later; a digital signature signs a hash of the message, not the message itself.

So, rule number three is:

Encrypting a message with a private key provides proof of origin.

The problem with asymmetric algorithms is that they are very computationally intensive and very slow. Asymmetric algorithms should not be used to encrypt large messages. That is why asymmetric cryptography is used to encrypt short messages such as a symmetric key or to encrypt a hash of a message as a digital signature.

Message Integrity and Hashing Algorithms

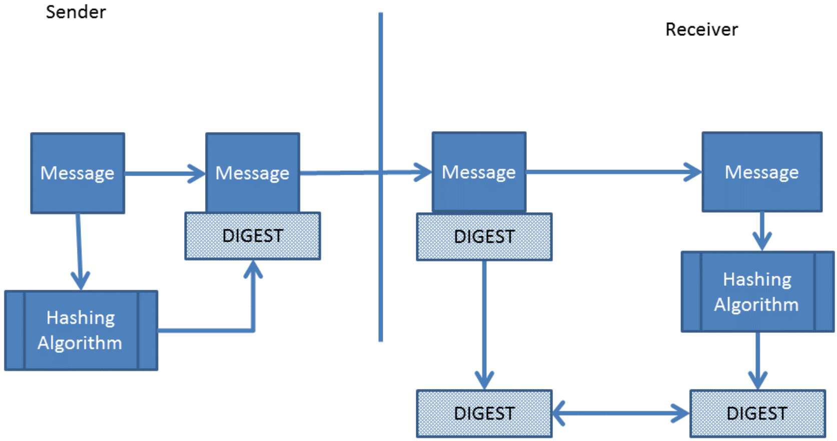
The earliest networks used by computers to communicate were based on older voice-grade telephone cable and were of poor quality, analog, and limited bandwidth. This meant that error-correcting was needed to ensure data integrity. This was originally done using methods such as parity bits, checksums, and Cyclic Redundancy Checks (CRC).

These methods were good to detect errors introduced by noise on the transmission line, but would not be effective to prevent a malicious individual from intercepting and altering both the message and the integrity value. In that case, the recipient would not realize that the message had actually been altered en route.

Hashing algorithms are a very good and accurate integrity check tool. Much more accurate than a checksum or parity bit, the hash will detect changes of even a single bit in a message. A hash algorithm will calculate a hash value (also known as a digest, fingerprint, or thumbprint) from the entire input message. The output digest itself is a fixed length, so even though the input message can be of variable length, then output is always the same length. The length depends on the hash algorithm used. MD5, for example, generates a digest length of 128 bits' SHA1, a digest of 160 bits, and SHA512, a 512-bit digest length. Those are the most common hash algorithms in use today.

When Alice wants to send a message to Bob and ensure that the message has not been affected by noise or network problems, Alice can, first of all, compute the digest of the message and send it along with the message to Bob. When Bob receives the message, he will compute the digest of the received message and ensure that the digest he computes is the same as the digest Alice sent him. As seen in the diagram below:

Fig 13 Verifying message integrity using a hash function

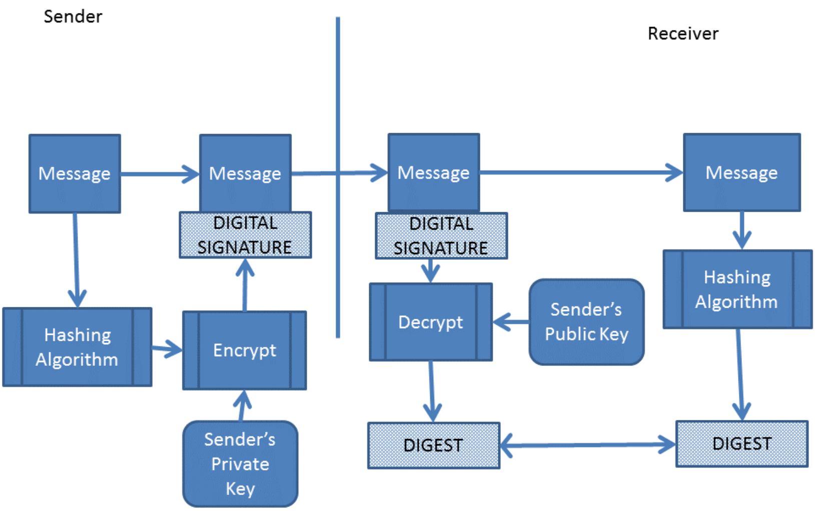


The problem with a simple hash operation like this is that the message and the digest of the message can still be altered by a malicious person in the middle of the transmission path. Therefore the solution is to combine two functions to protect both the message digest and to provide proof of the origin of the message.

Digital Signatures

A digital signature combines a hash function with asymmetric encryption. The hash function provides proof of integrity, whereas the process of encrypting the hash of the message with a private key does two things - it protects the hash from alteration and provides proof of origin of the message.

Fig 14 Verifying message integrity and proof of origin using digital signatures



As can be seen in this diagram, the message itself is not confidential. The purpose of a digital signature is to provide message integrity and proof of origin - not message confidentiality. Now, when Alice sends a message to Bob, Bob knows that the message came from Alice since he was able to unlock the digital signature with Alice's public key (and therefore, it MUST have been encrypted with Alice's private key). Bob also knows that the message he received is exactly the same as the message Alice wanted to send him because the hash of the received message is the same as the hash that Alice had signed.

Certificates

The purpose of a certificate is to link a public key with its owner. A certificate is usually generated by a trusted third party known as a Certificate Authority (CA). The CA generates a certificate on behalf of the owner of a public key that the owner can use to prove that this public belongs to them. If Alice sends Bob a certificate created and signed by a CA, then Bob can be confident that the public key in the certificate belongs to Alice. Then when he opens a digital signature with that public key, he knows that the message was signed and sent by Alice.

The format of a certificate is based on the X.509 standard. This ensures that certificates can be accessed by most browsers and systems and that the certificates are of a common format even though issued by different CAs.

A certificate is valid for a defined period (often one year). So Alice would need to go back to the CA on an annual basis to get a new certificate. However, if at any time, Alice wants to cancel the certificate, Alice will notify the CA, and the CA will put the certificate on a certificate revocation list (CRL).

PKI - Public Key Infrastructure

PKI refers to the implementation of asymmetric key cryptography. A PKI implementation is based on a CA that manages all the certificates for the members of the implementation group. Any member of the group can gain access to the certificates of the other group members. This ensures that everyone can communicate securely, knowing that their messages can only be accessed by the correct person. A PKI may use an external CA, or a company may be their own

CA and manage the certificates for their staff. Members of a PKI that belong to different CAs can sign a cross-certification agreement; this is in place for the members of one CA to be able to recognize the certificates issued by the other CA.

Putting it all Together

As can be seen, by the previous sections, cryptography has many moving parts and is a fairly complex series of operations. In many cases, we will combine several of these parts to accomplish various tasks.

Symmetric encryption algorithms are excellent to provide for the confidentiality of large messages but are difficult with key management. Therefore we will use symmetric algorithms to encrypt the message we want to send.

Asymmetric algorithms are very slow, but they are excellent to use for confidentially sending small messages. Therefore we will use them to send the symmetric key to the receiver of the encrypted message.

Hashing algorithms are excellent to ensure message integrity, so we will send a hash of the message to ensure the message is not changed en route.

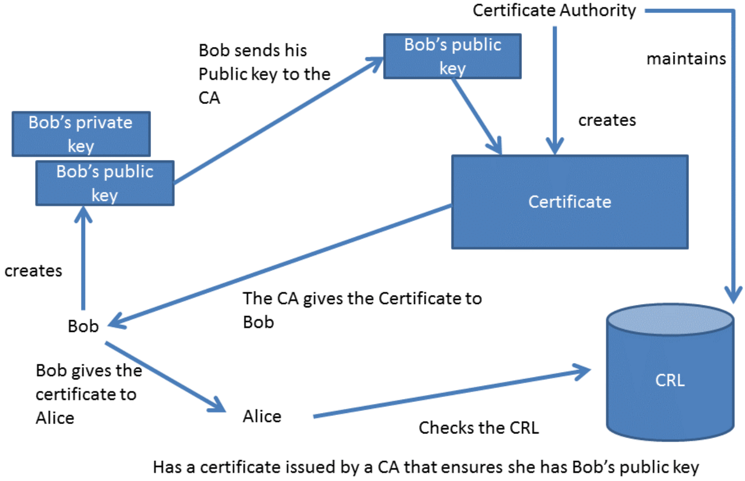
Asymmetric algorithms are excellent to prove proof of origin, so we will use them to sign the hash of the message - thereby creating a digital signature that can be used to prove both message integrity and proof of origin (non-repudiation).

Certificates provide assurance of the owner of a public key, so we use them to prove that we have the correct public key of the person or website we are communicating with.

The whole process can be seen here:

First of all, Alice gets the certificate containing the public key of the person she wants to communicate with (Bob). Alice validates that the certificate has not expired and that it is not on a certificate revocation list (CRL).

Fig 15 Certificate Authority


Certificate Authority
maintains
Bob sends his Public key to the CA
Bob's public key
creates
Bob's private key
Bob's public key
Certificate
creates
The CA gives the Certificate to Bob
Bob
CRL
Bob gives the certificate to Alice
Alice
Checks the CRL
Has a certificate issued by a CA that ensures she has Bob's public key

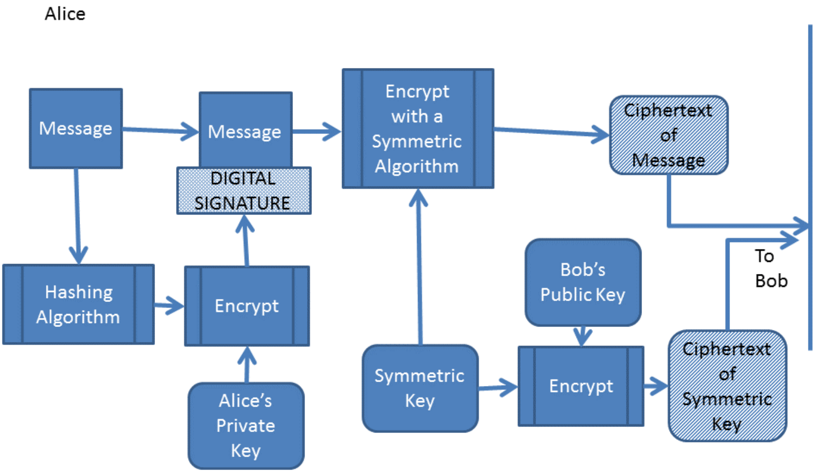
Then Alice creates a hash of the message she wishes to send.

Then Alice signs the hash of the message with her private key.

The digital signature is appended to the end of the message we wish to send to Bob. Then message (with the attached digital signature) is encrypted using a symmetric algorithm.

Then we encrypt the symmetric key used to encrypt the message with the public key of the recipient (Bob).

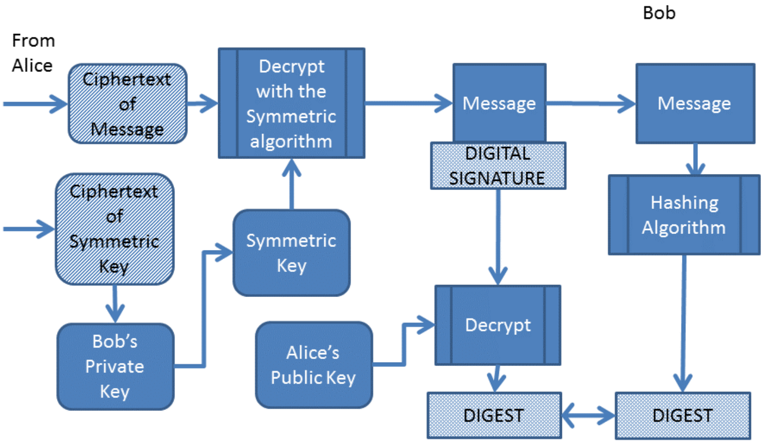
Fig 16 Using PKI for Secure Message Transmission
Provides message integrity, proof of origin, and message confidentiality



We send the encrypted symmetric key and the encrypted message to Bob. This is called a digital envelope.

When Bob gets the digital envelope, he will decrypt the symmetric key using his private key.

Fig 17 Decrypting a Secure Message and Validating Message Integrity and Proof of Origin



Bob uses the symmetric key to decrypt the message and the attached digital signature.

Bob decrypts the digital signature with Alice's public key and finds the hash of the message signed by Alice.

Bob creates a hash of the message he decrypted using the same has an algorithm that Alice used.

Bob compares the hash value he created with the one sent and signed by Alice. If the hash values are identical, then Bob knows he has an authentic copy of the message from Alice.

By this process, Alice can send a confidential message to Bob without needing to use an out-of-band method of secret key exchange. Bob knows that the message came from Alice and that the message is authentic and was not changed en route.

Cryptographic Attacks

Just as cryptography is valuable to protect data, a lot of effort goes into breaking the cryptographic protection that cryptography provides. There are numerous ways to attack cryptographic implementations.

Attacking the key - The secret to breaking most cryptographic implementations is to learn the key being used for the encryption and decryption of the message. The key may be discovered through a brute force attack - trying all possible keys, but that is not practical for most systems today - the time and resources it would take would be prohibitive.

Other attacks on the key can be made through linear and differential analysis and known-plaintext attacks. With those attacks, the cryptanalyst has copies of ciphertext and the corresponding plaintext, and by comparing the texts, learns some of the behaviors of the algorithm that can lead to the discovery of the key.

The key may also be compromised in transit, guessed through inadequate randomization, or stored in an insecure location. The easiest and most vulnerable attack, however, has to be social engineering. Bribery, idealism, coercion, romance, and deception are all tools used by social engineers to convince people to disclose cryptographic secrets.

Another way to attack cryptosystems is to find mathematical weaknesses in the algorithm, such as algebraic flaws that may allow a person to manipulate the cryptographic operation.

A cryptanalyst may make a cipher-text only attack that examines samples of ciphertext and attempts to decode the messages. They may also measure the exact timing and power used by the cryptosystem to do the encryption or decryption process and learn information about the behaviors of the system from that data.

Summary of Cryptography

The security manager should know the strengths and weaknesses of symmetric and asymmetric algorithms, the methods of message integrity, the purpose of certificates, and how the various components of cryptography are used and work together.

Access Controls

Access control can be described as the heartbeat of information security. It is through controlling access to our networks, facilities, equipment, and administrative functions that an organization is best able to preserve the security of its information.

Access control is usually divided into four sections; identification, authentication, authorization, and accounting (sometimes also called auditing). Each of these plays an important role in building a secure access control system and tracking the activity that takes place on the protected entity.

Access control is about allowing the correct level of access to authorized personnel, but not permitting unauthorized personnel or entities to access a system or make any modifications.

Identification

Identification is the unique method of distinguishing one entity from another. Each process, person, or entity that requests access to a protected entity should be uniquely identified in a way that allows the system to enforce the correct level of access but only to authorized personnel.

Methods of Identification

There are many ways to identify an entity. These can be broken into two primary methods - entity or user identification; and node identification and authentication.

Node Identification and Authentication

Node identification is to identify a location or a device, but not necessarily the user that is operating the device. This has been used in the past on wireless devices to filter out devices that are attempting to associate with a wireless access point by Media Access Control (MAC) address. Only devices that had their MAC addresses listed in the authorized devices list would be able to log in. In the mainframe world, the operator console was often connected to the CPU via a hardwired direct connection. This connection was known as a trusted path, and there were certain operations and administrative functions that could only be executed if the operator was physically sitting at that console. Many other systems and network devices have a similar connection through an administrative port that would restrict any changes to the configuration of the device unless the administrator was connected directly to the administrator port. This would prohibit any changes from the network and make it much more difficult for an attacker to manipulate the device configurations.

Another method of node authentication is through an IP address. Some systems will restrict a person from logging in unless they are on a recognized IP address. Some applications are also set to restrict operations to a certain CPU (central processing unit) serial number. This prevents a purchaser of an expensive software solution from running the software on unauthorized systems. However, this can be a problem with disaster recovery plans since the software will not operate at an alternate location unless the supplier/vendor or the software permits it.

User Authentication

The most commonly recognized form of identification is to identify individual users or processes that are requesting access to a system or other entity. User identification should be the creation of a unique value for each user - shared identities remove the ability to track the activity on the system to anyone user. This is especially a concern when administrators share identities and use those shared identities to perform high-level administrative functions.

Identification of a user may be through a user ID, account or customer number, badge, biometric value (in physical security implementations), or other values such as an email address. One of the most important elements of setting up a new user account is to have a secure, reliable process to ensure that user IDs are only given to the correct people and that the user IDs are set up correctly.

Maintaining UserIDs

The maintenance of user IDs can be a tough challenge for many administrators. It is often found that many user IDs that should have been deleted or disabled still exist on an organization's systems. These are user IDs that were given to employees, contractors, consultants, auditors, and other authorized personnel that no longer require that access. Of greatest concerns are the user IDs that have high-level privileged access. Many other user IDs may exist that are not required either, but they belong to customers and are low-level ids that do not pose a serious risk to the organization. When an employee or another person no longer requires access to a system, their user IDs should be disabled or removed. Leaving user IDs on the system may pose a risk since they could be used by another person or attacker.

Authentication

Authentication is the validation or verification of the identification offered by the user. An entity claims whom they are by offering an ID and that they are allowed on a system based on that ID. The next step is to verify that it is the correct person offering that ID - not just an imposter or attacker. This is the process of authentication.

There are three primary methods of authentication in use today, knowledge-based, ownership-based, and characteristic (biometric-based) systems. No single form of authentication is considered trusted on its own since each type of authentication can be bypassed. Therefore, all authentication implementations in use today recommend the use of at least two of the three factors (knowledge, ownership, characteristic). The use of two of the same factors (a pin and a password) is not considered to be two-factor authentication.

Knowledge

Knowledge-based authentication uses a "secret" value as the authentication method. The most version of this is a password-based system that requires the user to know the confidential password to authenticate themselves to the system. The problem with a password-based system is the threat of replay attacks. Since the password remains the same over some time, an attacker that learns the "static" password would be able to log in as the legitimate user at a later date/time. Ideally, the password should be set up according to good password rules. A mix of upper and lower case letters, numbers, special characters, and not be repeated or reused.

Other forms of knowledge-based systems use Personal Identification Numbers (PINs), secret questions (although in many cases the question can be answered through a quick Google or Facebook search), and graphical passwords where the user selects an image that they associate with.

Ownership

The use of smartcards, tokens, RFID (radio frequency identifier) badges or other items represents the principle of authentication by ownership. Tokens are usually used to generate one time or dynamic passwords - a password that is only used once and then discarded so that it cannot be used in a replay attack even if an attacker learns the password. Ownership based systems may be very simple such as a scratch card or very expensive systems with card readers installed at each workstation. Tokens and smartcards are usually either synchronous or asynchronous working on either an event or time based or challenge-response scheme.

Synchronous Tokens

Synchronous tokens use a token that is in sync with the authentication server (AS). The AS knows the value on the token and will permit access to the user if the user provides the correct value. In many cases, the user must enter a PIN number (sometimes using the employee ID number) to activate the device. Synchronous tokens are usually either event-based or time-based.

Event-based Synchronous Tokens

Event-based tokens generate a new random value each time the user presses a button or requests a new value. When a user attempts to log in, the system will challenge the user for the next value generated by their token. The user will request that value from the token and supply it back to the authentication server. If the value is correct, access will be granted.

Time-based Synchronous Tokens

Time-based tokens generate a new random value every few moments. The user is required to provide the current value on the token to the authentication server. If the input value is incorrect, then access will be denied.

RFID

The use of RFID is increasing as more organizations realize the benefits of using small embedded chips for identification and authentication. It is simple to track movements of materials, employees, vehicles, and stock using small chips that respond to a query from an RFID reader. These chips are buried (embedded) into shipping containers, product labels, animals, and ID cards. The use of RFID can make tracking and inventory management easier and can be used to identify genuine versus fake products.

Asynchronous Tokens

Asynchronous tokens operate on a challenge-response scheme. When a user attempts to log in, the authentication server will send a challenge. The challenge is a random value, and the user must then input the challenge into the token and respond to the authentication server. In some cases, the challenge value sent by the AS is called a nonce - which stands for 'number used once.'

Characteristic - Biometrics

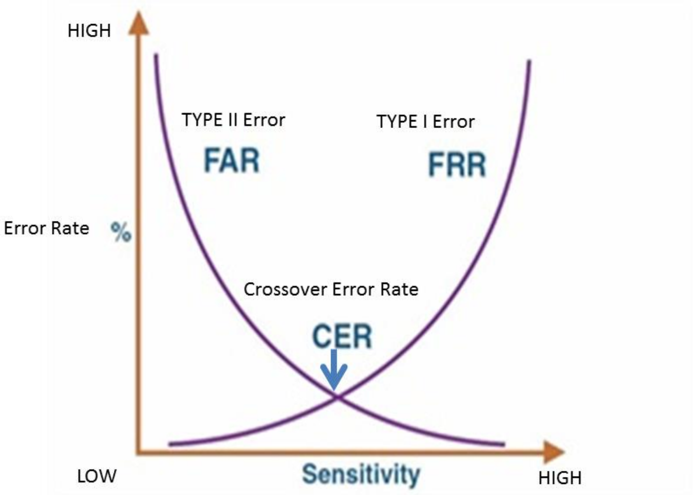
Biometrics is undoubtedly the most controversial form of authentication. Biometrics can be intrusive and may disclose health or other personal information and may evoke resistance amongst users. It has happened that putting in a biometrics system actually decreased the level of security in a facility since the users resisted it so much that they worked to circumvent the system.

A biometric system measures one or more unique physical characteristics of a user. These may range from fingerprints and palm scans to retina scans, iris scans, and handwriting style. The choice of biometric device is dependent on several factors, including costs to purchase, install and operate, the impact on productivity, and acceptance by the user community.

The use of biometrics in a technical sense has usually been to authenticate a user. However, when used for physical security, biometrics is often used for identification. The difference is in whether the user provides some identification to the system which is then validated using biometric data or whether the user is identified by the system from a list of known biometric values.

Biometric systems, like all other systems, are subject to error. The errors on a biometric system would be to grant access to an unauthorized person or to deny access to an authorized person. Of the two, the granting of access to an unauthorized person is more dangerous. This is called a Type II error. Denying authorized person access (thinking that they were an imposter) would be more of an inconvenience to the user than a serious risk to the organization. This would be called a Type I error. Most biometric devices have the capability of adjusting the sensitivity or precision of the device, and adjusting the sensitivity will affect the error rate accordingly. A device set for low sensitivity will have more False Acceptance errors and fewer False Reject Errors. As the sensitivity increases, the number of False Acceptance Errors will decrease, but more authorized persons will be subject to a False Reject Error. At one point, as seen in the diagram below, the two error types will intersect. This point of intersection is known as the Crossover Error Rate (CER) or sometimes as the Equal Error Rate (EER). This is the setting at which the device will have the lowest overall errors. However, in a very secure facility, the device may be set to a higher sensitivity to reduce the number of False Acceptance Errors to a lower level.

Figure 18 Biometric Errors



Authorization

Once a user has been authenticated as a legitimate user, the next step is to assign them the proper level of access to the system. Authorization is based on the principles of “least privilege” and “need to know,” and uses access control processes such as separation of duties, dual control, temporal access, and mutual exclusivity to ensure that a user only has the appropriate level of access to the assets of the organization.

Need to Know

Need to know is the principle of only granting entity access to the information that they require and hiding any other unnecessary information from them. This is often done with credit cards by only letting a merchant see the first six or last four digits of a credit card. Those digits are not protected and can be displayed, but the merchant does not need to see the remaining digits. By hiding (masking/obscuring) that data, the merchant is unable to misuse that information that they did not need to see anyway.

Least Privilege

Least privilege is the concept of only granting an entity the lowest level of access that they require to perform their job duties. For example, granting "read-only" access instead of "read/write."

Temporal Access

Temporal refers to "time" based access restrictions. For example, when user accounts are set up, a user may only be able to log in at certain times of the day. Their accounts will not work at other times. A user attempting to log in late at night or over the weekend would not be able to log in. This prevents the misuse of accounts by either the user or another person (cleaning staff) during non-standard operating hours.

Separation of Duties

Separation of duties is the practice of ensuring that no single entity has complete control over a sensitive transaction. For a transaction to be completed, it would require the participation of more than one entity. This is accomplished by breaking a job into separate parts and having different people execute each part. An example of this is processing expense forms. An employee can submit an expense form, but it must be reviewed and approved by another person before payment. In many cases, even the payment process is further subdivided into that another person must sign the check or initial the cash disbursement. Separation of duties is used to prevent and detect fraudulent activity, or to catch errors before they are submitted into production.

Mutual Exclusivity

Mutual exclusivity is closely linked to the separation of duties. When a transaction is divided into several separate tasks. Each task must be executed by a different person. One person mustn't just do each task, thereby circumventing the separation of duties.

In many cases, a person may have the right to submit work, authorize the work of others, and perhaps even correct errors. But even though any one person has the rights to both submit and approve those two tasks are mutually exclusive. If they submitted the data, then they would not be allowed to approve it. If they approved the work of someone else, they would not be able to correct any errors. This can prevent fraud and also help ensure that any errors are detected by having someone else review the work of their peers or subordinates.

Dual Control

Dual control is the real-time practice of implementing separation of duties. Whereas mutual exclusivity implements separation of duties by having different people involved in a sequential series of activities. Dual control often requires two separate people working together simultaneously to complete a task.

Location-based Access

When a user logs in from their desk - a more controlled environment - then they may have their full access rights, but if they log in remotely - from an uncontrolled environment, then their access may be more limited. It could be that they are unable to download any data or access more sensitive information when at a remote location.

Levels of Access

The levels of authorization are based on the principles listed above, according to the requirements of the user. Some users may be administrators and have nearly unlimited access, while others may have read-only or write-only access. The term sometimes used is CRUD (Create, Read, Update, Delete). The level of access granted should only be according to the job requirements, and the user should use that access with an awareness of the policy, procedures, and responsibility that comes with access.

When an administrator has an account with high-level access, they should use that account sparingly and have another less privileged account that they use for normal activity. Of course, all activities done at the administrator level should be logged and traceable back to the individual administrator. These logs must be reviewed to ensure that no unauthorized changes have been made.

Accounting / Auditing

Accounting or auditing is tracking and monitoring all the activity on a system and being able to associate that activity with the entity that performed that activity. This is one reason that User IDs must be unique and able to be linked to an individual person or process. The accounting process creates a log of all activities that can be used in investigations, review, and training purposes.

The logs should record all activity on the system. All administrative changes were made, login attempts, and any errors that occurred on the system. Since the logs will often contain sensitive information or reports on improper activity, the logs should be protected from unauthorized access or modification. Even administrators should not have the authority to changelog files.

Some organizations will use clipping levels to reduce the amount of data in a log. A clipping level sets a threshold for activity and will not record repeated errors or take action until a certain threshold has been reached. A user, for example, that tries to log in with the wrong password will not be locked out after only one attempt, but will instead be allowed to try three or four times before locking out the account.

In this case, the threshold is set to represent the difference between normal human error and what could be a malicious attack. A user should be able to log in correctly within three or four tries. If they cannot, then it is probable that they will not remember their password. This saves the helpdesk from too many random passwords reset requests just because someone mistyped their password once or twice.

Many privacy laws today require an organization to maintain a sound system of record (ASOR) for any person that accesses private information. This is used to identify anyone looking at data that they do not need to be looking at as a part of their job responsibilities.

Identity Management

The world of identity management is much more complex and challenging than it was a few years ago. Before the development of websites and online services, the only people on the systems of an organization, with a few exceptions, were its own employees. Employees were people the organization could train, monitor, and, in some cases, discipline. Nowadays, most of the users on an organization's systems are customers, clients, or business partners.

And in most cases, they are logging in from systems that cannot be trusted. Sometimes even over an independent and vulnerable network (the internet) and may be located anywhere in the world and, therefore, not even subject to the same laws, ethics, or cultural standards. These are people that cannot be controlled, and it is impossible to enforce most security standards that would be mandated for the employees of the organization.

The challenges related to identity management apply at all levels of the security model - at the hardware, network, application, database layers, and in all departments and across all lines of business. This requires a unified approach to managing the identities of the users that sets out consistent standards for all users of all systems and from all locations. A poorly set up access on one system could easily translate into a security breach on other systems.

One of the most substantial challenges is related to password management. This includes teaching users to select good passwords, keep them private, and not to use the same password for online banking as they apply for email. When resetting a password, the organization does not want to employ a large staff on the helpdesk just to reset user passwords daily. The company needs to have processes in place to ensure that a password reset is only granted to the correct user, not to someone masquerading as the legitimate user.

There needs to be a clear separation between users of different levels of access. This requires a system of multi-level security that is hard to design and even harder to preserve in today's complex world. There are many opportunities for covert channels or ways to bypass the security controls and find that information is accessible to people with the wrong level of privilege.

As internal users move around within an organization, we often see the development of "access creep" where a user's access permissions accumulate over time, and they are just granted more and more accessible as they move from one department to another. This is why all managers should be required to review, sign off, and be accountable for the access levels of their staff on an annual basis. The access controls should also be enforced in a standard manner so that new users are set up, user permissions are maintained and reviewed, and old UserIDs are disabled or deleted when no longer required.

The challenge of identity management has led to the development and implementation of several single sign-on solutions.

Single Sign-on

There are many types of single sign-on solutions, but they all have similar goals - to help manage system access consistently and measurably. A single sign-on solution is, by its nature, a centralized access control solution since it maintains access to multiple systems.

Centralized Access Control

Centralized access control is the principle of managing access to all systems and networks from a central location, or by a centralized department. There are many advantages to a centralized access control system:

1. Access is consistently managed; access permissions are easier to monitor and review.
2. Access levels are enforced on all systems in the same way.
3. For example, the same number of invalid login attempts before the lockout.

However, centralized access control systems also have disadvantages in that they can be inflexible, unresponsive to local requirements, be a single point of failure, and bureaucratically heavy.

With a centralized system, all access requests must be submitted to a central department, which then sets up, or removes, the access permissions according to the policies and access control procedures of the organization. This prevents a local office from setting up access permissions according to a local, inconsistent process.

A centralized system can be set up to manage access as a front end portal or as a backend authentication server using a product like RADIUS or TACACS+.

Decentralized Access Control

Decentralized access control is when a local office or system owner has the authority to manage access permissions directly. This is an ideal solution for an organization that is quite spread out, with many local variances and local operating environments. This method is flexible to local needs, quickly responsive, and much less bureaucratic. However, it is rife with security flaws - a manager may just grant too much access to staff, may violate privacy laws, may set up access inconsistently, and may not review access permissions or logs regularly.

Federated Identity Management

Many organizations today use federated identity management to allow customers to log in once to a trusted business partner and then access the systems and data from other partners in the federation without having to log in repeatedly to each partner. This process uses the Security Association Markup Language (SAML) and security artifacts to manage user access. This makes the interaction between the user and the web-based services of an organization much more user-friendly and streamlined. Though, the members of the federation must have a way to trust one another to make it work effectively.

Web Portals

Web portals act as a front end to many services behind the portal. An organization, such as a bank or government, provides many different types of services to its clients/citizens. Instead of having different web pages that a client must separately go to for each individual service, the bank sets up a front end page that acts as the entrance or lobby for the clients.

From that page, they can log in, and they can select various services. Through the use of cookies, their preferences can be "remembered" so that the web page is configured according to their preferences on future visits. Whereas a federated system links different companies together, a web portal is often linking various services of one company together.

Script-based Sign-on

When an individual logs on to an information system, the system executes a logon script that requests the login ID and password from the user. Originally every system was built with its own login script, and the user was required to log in separately to each system. The script-based single sign-on system puts a front end application in front of the older legacy systems that the user logs into. Then the application executes the scripts in the background to allow the user to log into each of the individual systems "hidden" behind the single sign-on application.

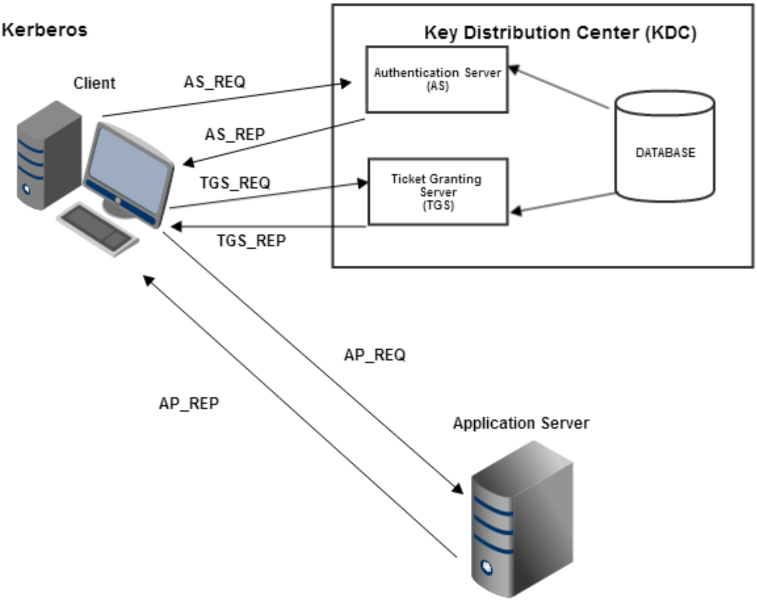
Kerberos

In the mid-1970s, MIT developed a project known as Athena, to manage single sign-on. Today this is known as Kerberos and is built into many of our available systems. Kerberos is a single sign-on product that manages all access for users and devices on a network. The heart of Kerberos is the KDC (Key Distribution Center). The KDC is comprised of two parts - the Authentication Server (AS) and the Ticket Granting Server (TGS).

When a new user or device is attached to the network, it must be registered with the KDC. At that time, a symmetric key is chosen for the user/device and stored both on the KDC and the device. A user requests access to a device or application by sending a request encrypted with the user's symmetric key to the KDC. If the user is permitted access, then the KDC passes a time-based ticket back to the user along with a symmetric session key. The user then passes the ticket (which is encrypted with the symmetric key of the application) to the application.

The application can read and verify the ticket and then use the symmetric session key to communicate with the authorized user.

Fig 19 Kerberos

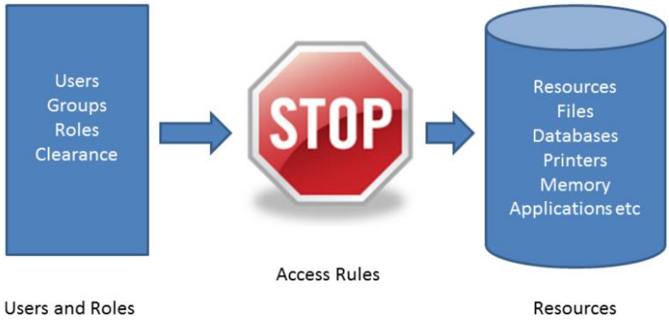

Key Distribution Center (KDC)
Client
AS_REQ
Authentication Server (AS)
AS_REP
DATABASE
TGS_REQ
Ticket Granting Server (TGS)
TGS_REP
AP_REQ
AP_REP
Application Server

Kerberos has the weakness of being vulnerable because it does not recognize a brute force attack against the stored passwords. The KDC is also a single point of failure and must be redundant, physically protected, and carefully administered.

Access Control Methods

There are many ways to implement access controls. In a physical sense, a person can have certain rights or capabilities. For example, they may have an ID card that indicates which buildings they may enter. There can also be a list of which people are allowed access to a certain area. In both cases the information is the same - it is the list of who can go where and what can they do - the only difference is that one looks at the permissions from the perspective of the user, and one from the perspective of the protected asset/building. This is the concept of an information management model (IMM). An information management model describes the relationships between subjects and objects and the rules that must be set up to manage that relationship.

Fig 20 The Information Management Model



The information management model starts by identifying all users and all objects and then documenting the rules that will be enforced between those entities.

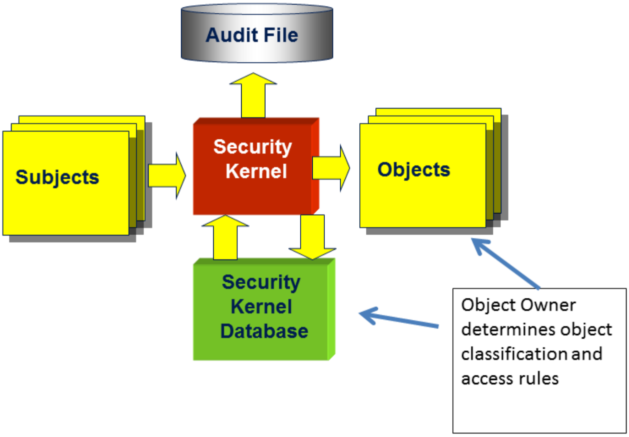
Subjects

A subject is an entity that requests a service from another entity. For example, a user trying to access a building. Since the subject initiates the activity - it requests access; it is considered to be "active." Most subjects will have a level of clearance or permissions that indicate what they are permitted to do. Examples of a subject would include users, clients, programs, processes, and applications.

Objects

Objects are the protected asset that provides the requested service to the subject. A subject asks for something - the object then provides the service as requested. Since the object does not initiate the activity, it is considered to be passive - it will remain in its current state until it is acted upon by a subject. Examples of an object would include files, databases, memory, printers, networks, applications, processes, programs, books, and buildings, to name but a few. Some entities may be either a subject or an object depending on the situation. A user may access a program - in which case the user is the subject, and the program is the object, or a program may want to save data to a hard drive in which case the program is the subject and the memory the object.

Fig 21 Reference Monitor



Reference Monitor

The diagram above is the same as the Information Management Model diagram except that now we have replaced the "Rules" with the mechanism that will enforce those rules - the reference monitor. The reference monitor is just a concept - the idea that represents the enforcement mechanism. The concept of the reference monitor (it monitors a request by a subject to reference an object) is implemented through an access control mechanism - such as a security guard that protects the entrance to a building.

The security guard enforces the rules provided by the "owner" of the facility and ensures that only authorized personnel are permitted to enter. The guard may require some form of authentication - through an ID card or biometrics before allowing a subject (the person) to gain access. The security guard may also log all activity - who enters and leaves, who signed in a visitor, who tried to enter but was refused - all of these can be logged and used for future investigation, if necessary. It is important to remember that the security guard only enforces the rules given by the owner. The security guard is NOT responsible for determining who should and who should not have access - only the owner can decide who should be let in, and what procedures must be followed to enable that access. Several simple and logical rules must apply to the reference monitor. The rules are:

1. The access control system must mediate ALL access - in other words, whenever an entity desires to access. It must intercept the access request, verify whether that access should be permitted and then grant (or deny) access according to the rules provided by the owner.
2. The access control system must be testable; there must be a way to validate that the access controls are working correctly and only allowing appropriate access to authorized personnel.
3. The access control system must be protected from modification or tampering - no one should be able to change the access control rules except through an authorized process. The entity requesting access (the subject) should not be able to change its own rules).

Implementing Access Controls

Access controls are implemented through a variety of methods ranging from physical security measures such as locks and guards, access control lists, capability tables, and directories.

Access Control Lists and Matrices

As one of the most common forms of access control for information systems, an access control list is quite simply a list of the rights or permissions granted to a subject to an object. In most cases, it is a list of all objects and what permissions various subjects would have to read, write, execute or delete that object.

This can be written in a list or in a table that shows the relationships between all the subjects and objects.
The list can also be created from the perspective of the user, which states what rights a user would have - for example, what files or applications can they access. These are frequently called capability tables.

A directory is a type of access control list that often groups users together that have similar access requirements.

Rule-Based Access Control

Firewalls are an example of a rule-based access control system. A firewall has clear, explicit rules about what types of traffic it will allow or disallow. These rules are then enforced to all the traffic going through that firewall. A similar approach can be used with access controls to a system or network. Rules that will enforce the access permissions given to any individual entity can be set up.

Role-Based Access Control (RBAC)

Role-based access control is an excellent method of controlling access to groups of users that have identical or similar access control requirements. Users are grouped into job roles, and the appropriate access permissions are granted to those roles. Any user enrolled in a role will inherit the rights and permissions of that role. This system works well when the user population is dynamic, with many users having similar requirements but with a lot of staff changes.

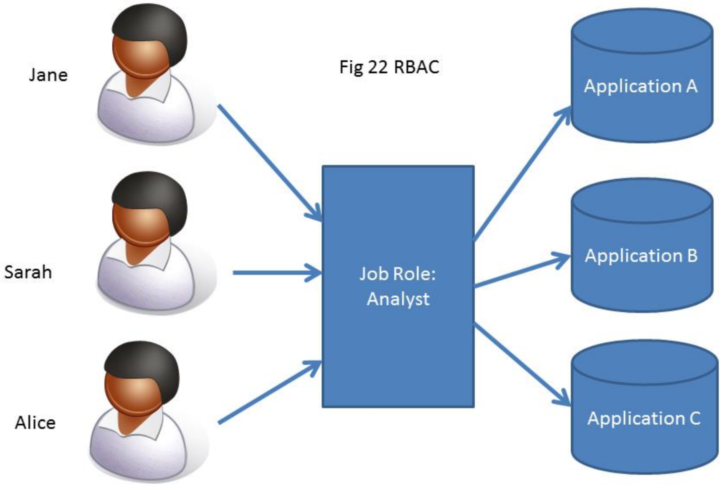


Fig 22 RBAC

Assurance

Assurance is the measure of trust or confidence in the effectiveness of the security controls. In this case, assurance would be proof that the information classification and handling procedures are being followed and protecting the information. Some of the common assurance mechanisms include checking the labeling and handling of the data.

Access Control Theorems

There are two primary theorems used concerning access control systems. These are Discretionary Access Control (DAC) and Mandatory Access Control (MAC). These refer to the principles of policy, procedures, and system and data protection. These terms have been used since the 1970s as ways to describe information access control theories.

DAC

Most of the access control systems in the world are DAC. DAC systems are used in physical access, network access, and system and application access as an easy method of enforcing appropriate access control rules as determined by the asset owner. Whether or not access is granted is at the discretion of the owner. It is up to the owner to decide who should or should not have access, what level of access they should be granted, and ensure that the rules are set out to manage access permissions correctly.

In a DAC system, the rules are set by the owner and enforced by the access control system itself.

MAC

Mandatory access control systems are rarely found outside of military and intelligence networks. MAC systems are very expensive to set up and maintain and require substantial physical and procedural controls.

A MAC system still requires the consent of the asset owner to grant permissions, but the second level of access controls based on labels also must be satisfied, or access will not be granted. The labels are based on the classification of the object (set by the object owner) and the clearance of the user (usually set by a security administrator). This supports the separation of duties and is a check and balance to ensure that access would not be granted in error or in violation of policy by the owner of the system.

The principles of MAC and DAC were outlined in the old Orange Book (TCSEC) that set out the criteria for evaluating the security of information systems.

Attacks on Access Control Systems

Every system must be built with the expectation that it will be attacked. This especially applies to access control systems since they manage access to most systems and provide the point of an attack for an unauthorized user attempting to gain access. There are many types of attacks - from password cracking to physical penetration, and from low-level social engineering to highly technical advanced persistent threats (APTs).

Password Cracking

One of the easiest ways to penetrate a system is by learning the password of an authorized user. This can sometimes be done with little or no technical skill since many users do not realize the importance of keeping their password secret. A part of every awareness program should be to remind users that the reason to protect their password is so that they will not be blamed for something someone else has done using their account! Users often write passwords down or choose weak passwords that can be easily guessed or broken. Over the years, numerous password cracking tools have been available such as 'lophtcrack' and 'john the ripper.' Today there are many ways to circumvent a password using tools such as Cain and Abel, or Helix.

Dictionary Attacks

Many people choose a password from a list of common words. Even if they exchange some number for letters, (3 for 'e,' 0 for 'o,' etc.,) most dictionary-based password tools will make the same substitutions. A dictionary attack is based on a list of common words that the tool will hash to attempt to find a matching password hash value in the password file (SAM file for windows).

Since a password is usually stored as a hash value and not usually stored in cleartext, the dictionary attack tried to find the word that, when hashed, will give the same hash value. The attacker then knows what password they must enter to log onto the system. This is one reason to protect the password file - to prevent an attacker from taking a copy of the file and running an attack against it to learn the password values.

Brute Force

The brute force attack is based on trying all possible values to get an input password value that will give the same hash as a stored password hash. In some cases, the input will not be the same as the real password, but instead, it will be a value that generates the same password hash. This is called a collision. A brute force attack takes a lot more time than a dictionary attack, but given enough time (maybe years) and resources, a brute force attack would always be successful.

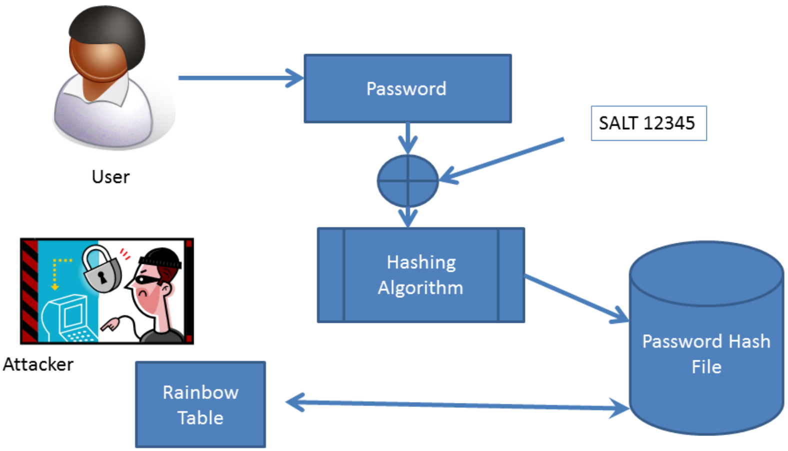
Rainbow Tables

There are several versions of rainbow tables that are available on the internet. These are tables of pre-calculated password hashes and the input value necessary to generate that hash. If an attacker can obtain a copy of the password file, then they can quickly look up the hash value in the password file and instantly cross-reference the password hash to a value that will generate that hash. This technique, an unsalted password, can be broken in very little time.

Salts

A salt value is a value added to a password before hashing. This will obscure the true password so that it is not easily broken using a dictionary attack or rainbow table. The stored hash value is a combination of both the salt and the password, so the values in the rainbow table will not generate the same password hash as the user's password.

Fig 23 SALT Values



Other Methods of Defeating Access Controls

Access controls can also be defeated through gaining physical access to network cabling, network devices, or servers; through exploiting a vulnerability such as SQL injection or planting a rootkit on a system.

Summary of Authentication and Access Controls

This is a critically important domain, and many-core principles and concepts were covered in this domain. The security professional should be familiar with Identification, Authentication, Authorization and Accounting, role-based access control, DAC, MAC, information classification, and single sign-on.

Human Resources Security

People and Security

An organization can have the best tools, the best policy, and the most up-to-date technologies - and still, be a victim of a security breach. That is because, in the end, security is primarily a people problem. It is people that will either make or break a security implementation. Whether by accident (error), negligence (taking a short cut or bypassing procedures), or intention (overtly bypassing an organization's security), most security breaches can be tied to a people-related problem.

Skills

Security is not a naturally known skill and requires training, awareness, and diligent monitoring. Naturally, most people would rather deal with trust or ease of use rather than in fear, caution, or taking extra steps to ensure security. When a person has a responsibility, they need sufficient training to be able to execute that responsibility effectively. No one can be expected to do a good job of something that they know little or nothing about. This especially applies to the use of information security tools.

There are many excellent tools available to an organization today, ranging from next-generation firewalls to Intrusion Detection and Prevention systems, switches and routers, to testing tools and monitoring devices. Many of these devices were either built specifically for security or have security functionality capability. The challenge seen in so many organizations is that these controls are not being used effectively.

Devices are misconfigured, security functionality is not enabled or is enabled incorrectly, devices have overlapping control capability, but either device is operating correctly. Most systems and network administrators are so busy dealing with immediate business needs that they are oblivious to security issues or threats. For several years already, it can be seen in the annual Verizon Data Breach Report that 96-97% of all security breaches could have been avoided through the implementation of simple controls - well-known and effective controls. So the question is. "Why do we still see these security lapses, even by large organizations that spend a lot of money on security, nearly every week?"

The answer has to come down to people. The tools are there but not used effectively. In many cases, it comes down to training. Staff is expected to maintain or operate a system that they have never been adequately trained on. When a new device is first implemented then training may or may not have been provided, but in the time since the implementation, the people originally trained have moved on, and the new staff has not been provided the training, nor the time, to learn how to use the device effectively.

Hiring

It has been reported that as many as 80% of all resumes or Curriculum Vitae (CV's) contain errors or misstatements. These errors may be incorrect listings of experience, certification, education, or responsibilities. When an organization hires a new employee or even engages a contractor or consultant, it is important to verify the claims made in the application and determine whether the prospective employee actually has the necessary skills to do their job. An organization may also want to perform criminal record checks on an employee that may be in a trusted position.

Termination of Employment

When an employee is leaving the organization, it is critical to remove their access. Ensuring that if they have been able to use their own devices that no corporate data is remaining on the device.

Conducting an exit interview with a departing employee can also be a good manner of gathering information about strengths, weaknesses, and possible improvements that can be made to the organization.

When an employee or contractor leaves under involuntary terms, it is often advisable to escort them off the premises and ensure that all access accounts are disabled immediately.

Social Engineering

Social engineering is the manipulation of people to commit illegal or unauthorized activity. Social engineering is one of the most serious threats today. In many cases, the way an attack was successful was through the manipulation of people and the power of social engineering. There are several forms of social engineering, including Name-dropping, Intimidation, Appealing for help, and Technical.

Name-Dropping

Name-dropping is used to convince an employee that another person has authorized them to do something for the supplicant. For example, a person calls up to an administrator and states that the administrator's boss has authorized the supplicant to have access to a system or network and said that the administrator would set this up.

Intimidation

Intimidation is the act of threatening a person to commit an unauthorized action. This is often done by threatening to escalate to a manager, threatening the job of the employee that is not willing to break the rules or even threatening the family of the employee.

One of the reasons that this is so successful is that many managers also do this and expect a different form of treatment than other staff gets. For example, a manager may not think that they have to show or wear an ID card to obtain entrance to a facility. A person that would challenge the manager to show their card would be at risk of losing their job. Such action creates a fear that can be exploited by an imposter that claims to be a manager and, therefore, is affronted that anyone would dare challenge them.

Appealing for Help

Appealing for help is playing on the emotions and natural desire of many people to want to help out a person that is struggling with a problem. An attacker calls a help desk expressing problems with accessing certain data that they desperately need for a report for management, and ask for help as to why they cannot seem to get it to work. The help desk falls for the story and grants them access or else provides the information the attacker wanted.

Technical

Many attacks today are based on phishing attacks, the so-called 419 scams, phone-based scams, and other technology-based methods. Originally many of these came via fax messages or calls purporting to be from official demanding information. Today, they often threaten that online banking access will be cut-off, or that fraud has been seen on a person's account and require that person to provide personal information to prevent that fraud.

The Cure for Social Engineering

There is **no cure for social engineering** except to repeat, over and over again, that social engineering attacks and email claims of lottery winnings or fraud alerts are all false and must be disregarded. It is similar to the way of dealing with childhood disease through vaccinations, give people an information session that explains what social engineering is, how to react to a social engineering attack, and what the consequences are for being misled or not following proper procedures. But even with vaccination, it is important to have a repeat dose in many cases a few years later.

Training, Awareness, and Education

Employee development takes many forms - from annual reviews to job action plans, and from training to education. There is little doubt that one of the best investments an organization can make is to invest in its employees through training and education. People need the right skills to do their jobs, and they need to be challenged and encouraged to keep up their skills and qualifications. Too many people lose their jobs today, and because they have not kept up their skills, it can be very difficult to find a new job. A lack of commitment to the organization or lack of expertise to maintain the systems and networks of the organization puts the entire organization at risk, not just a single system or department.

Training provides the specific skills and knowledge needed to implement, operate, and maintain a system, device, or application. Education is more well-rounded, often based on soft skills or more general knowledge that can be used to manage or assist in decision-making.

Security Awareness

Perhaps the most powerful tool in the arsenal of the security professional is a strong security awareness program. Security awareness provides the general knowledge to everyone in an interesting and informative manner. Awareness training ensures that everyone knows the policies, ethics, procedures, and security culture of the organization.

Once people are aware of the threats, vulnerabilities, and risks faced by the organization, they are better prepared to make the correct decisions. They can work together with the security team to help protect the organization, rather than possibly be the person that makes a mistake leading to a serious breach.

The policy is nothing but good words if they are not backed up by action. Policy needs to be implemented through procedures and standards, and the contents of the policy must be communicated to all staff. The policy is of little value if no one knows it exists. Therefore, the main objective of security awareness training is to ensure that everyone is aware of the policy and knows what their responsibilities are. Security is the business and a requirement for all staff, and all staff must work together to enforce, monitor, and promote the policies of the organization.

Delivering an Awareness Program

Awareness programs have a well-deserved reputation for being boring lectures about choosing stronger passwords (defined by Bruce Schneier as a password that impossible to remember but should not be written down) and trying to sell a security through fear, intimidation, and uncertainty. This approach creates an "us versus them" mentality. It encourages the thought that security is working against the rest of the workforce instead of working with them for the betterment of the organization.

Awareness training should be multi-faceted - interesting, innovative, varied, and challenging. The message should be tailored to the audience at the level understood, applies to the audience, and addresses the actions that specifically apply to those in attendance. Using different media - such as posters, handouts, brief messages, login screens, humor, real-world examples, and rewards in the awareness program can appeal to the audience and pique their interest.

When security awareness sessions have been completed, it is good to review the effectiveness of the programs. Has the message been understood? Did the session change the attitude and behaviors of the staff? Was the core message clear and unambiguous? This can be done through surveys at the end of the session, but those may be of limited value. The most important result of an awareness session is the effect the session has on the attitude and behaviors of staff. Therefore, one of the most important measures is whether the staff does believe the message and follows up with better security practices. Sometimes just checking how many people went back to their desks and changed their passwords after an awareness session can be a good measure of the effectiveness of the message.

Summary of Human Resources Security

Hire the right people and train them! This can be accomplished through a well-documented hiring process - that checks references, education, certification, and criminal history. Ensure that the staff responsible for maintaining systems and devices have been provided with suitable levels of training. Have a termination procedure to ensure that access is revoked and equipment is returned when leaving the organization. More importantly, ensure to delete corporate data from personal systems and equipment.

Provide security awareness training and monitor the effectiveness of the training.

Networks and Communications Security

Networks are the lifeblood of nearly every line of business today. It is through networks that applications, manufacturing machines, shipping, payroll, and finance all operate. Secure and reliable networks are required to provide communications services that are accurate, available, and confidential.

When protecting networks, it must be remembered that network defense has two components. The network itself must be protected against attacks that would disable or affect network operations; network defense must also protect the devices attached to the network since the network is often the mechanism used to direct an attack towards a network-enabled device.

A network is created when any two devices can communicate. Therefore networks can be as small as a personal area network - a person with a Bluetooth headset talking to the phone on their bed or a network can span the globe with thousands of devices all sharing the same network infrastructure.
Several models are used to manage network communications. The OSI (Open Systems Interconnect) model is the ISO7498 standard. The OSI model divides the process of communications into seven layers - each layer with a defined purpose and function. As each layer fulfills its purpose, it wraps the data to be sent to the layer above or below it in a process called encapsulation. Each layer can perform its function independently of the other layers.

The layers are as follows:
Application - the layer that interfaces with the application being used by the user. It is not the application itself. This layer

ensures the data is in a format that can be transmitted over a network and understood by the system at the far end.

Presentation - this layer is used for protocol conversion and compression-decompression of the data.

Session - this layer manages the session between the two endpoints - login, authentication, and identifying the packets of information according to each session.

Transport - this layer manages the end to end transmission of the data. TCP ensures that all packets are received. When using UDP, the transport layer enables fast, low-overhead communications but without any form of error control or proof of delivery.

Network - the network layer moves data across networks with the best-effort approach. The most common protocol used here is IPv4, which places a 32-bit address on the packet to enable routing the packet across the network. Over the next few years, IPv4 will be replaced with IPv6 - with a 128-bit address space. Currently, IPv6 has a limited deployment - mostly being used for backbones and another inter-ISP routing.

Datalink - this layer connects two physically adjacent devices - it provides the interface between logical and physical addressing (Ethernet addresses, for example).

Physical - The physical media is the actual manner of connecting adjacent devices over various types of media - wireless, fiber, copper, etc.

Over the years, the way of communicating across networks has changed dramatically. Early communications were based on the public switched telephone network (PSTN), and messages were transmitted using circuit switching over voice-grade cabling. The [central] offices of the telecommunications providers in every part of each city and town were linked together through cabling, and the switches and multiplexing equipment in each office established the circuits used to carry communications traffic. The early forms of transmission were analog, which had limited bandwidth (based on the range of the human voice).

When computers first started communicating over the PSTN, a modem was required to convert the digital signal of the computer into an analog signal that could be transmitted over the existing networks. These were all circuit switching in that a circuit between the two endpoints was established at the beginning of the communications session according to the best route available at the time. This circuit remained established as long as the two parties remained connected. When either party hung up, the circuit would be dropped. This form of communication worked very well for voice since it had a consistent level of latency (delay) and a fairly stable level of quality. But the voice was very tolerant of noise, whereas data is not. Data is easily confused by noise on the line, not knowing if the noise is legitimate data or not. Because of this, early communications for data had to include extensive error-correcting.

Instead of a modem, many companies then moved to a leased line. A line (circuit) that the company purchased from a telecommunications carrier that was dedicated to the company's own private use - hence the term private line was born to describe a circuit dedicated to the use of one customer. Even though the data sent over these private lines were digital, they were still operating over an analog-based phone system; therefore, their network speeds were quite limited.

The problems with a private line were cost and efficiency. The private line itself could still be a single point of failure. A cut cable would cause a denial of service on what may be a network connection that was critical for business purposes.
Then came the idea of packet-switched networks. Instead of sending all the data over a committed private line in one streaming flow of data, the idea was to divide the data into individual packets and send them individually over the network. This meant each packet had to have an address so that it could be routed toward its final destination.

Now the idea of moving to packet switching became possible. Instead of using the switches in the central offices to establish a fixed circuit for the traffic to route across, now each switch would operate as a cloud and allow each packet of traffic to flow across the network of switches in whatever manner was best at the time. This allowed much more efficient use of the cabling since each packet of traffic could take whatever path was available at the time, and the traffic from many companies could share the same communications channels instead of having an expensive dedicated private line. However, since different packets could now take different routes to the destination, new problems arose. Packets could arrive out of order. Packets could experience various levels of latency and arrive at various speeds, causing jitter. However, this is still fine for data. Data is well suited for bursty and variable traffic. By fragmenting data into individual packets and then buffering them at the far end, the data could be easily re-assembled.

The first real standard used for this type of communications was X.25. This is an excellent standard, especially for use with low-quality voice-grade cables. X.25 employed error protection at each point along the way, so errors would be corrected before the data was further down the network. X.25 is still in some limited use today, but it has been phased out of most regions of the world. It is limited to data only and cannot handle other types of traffic.

Then came the development of frame relay. A packet of data at the data link layer is commonly called a "frame," and the purpose of frame relay was to pass (relay) these frames over the network. In the meantime, a lot of the old poor quality cable had been replaced with fiber. This meant that the error-correcting feature of X.25 was no longer needed since error-correcting could be made at the endpoints instead of at each node along the way. This resulted in faster speeds.

Another technology was the development of ATM (asynchronous transfer mode). ATM traffic is divided into fixed-length cells instead of variable length frames. This also permitted better speeds and more efficient handling of the data. The introduction of these packet-switched networks did have a disadvantage in that traffic speeds were variable. For some organizations with defined business and network requirements, this may not be a deal. Just when the network is needed most, it may be very slow. The solution to this was to create a fixed path that the data of an organization would take through the packet-switched network. This would create a virtual circuit that would provide more consistent levels of performance. When this path or circuit was permanently set up, this was called a permanent virtual circuit (PVC). When the circuit was established as best available at the time of communication, it would be called a virtual switch circuit (SVC).

Many organizations chose to pay a premium to be guaranteed a certain amount of bandwidth for their communications. This is called Quality of Service (QoS).

Other developments in communications have included the development of Multi-Protocol Label Switching (MPLS). MPLS runs over frame relay or ATM. It allows engineering of the traffic, including defining the route the information will travel, QoS, and CoS (class of service) where different types of packets can receive priority handling - voice getting priority over data, for example.

Physical Media

There are many ways to connect devices today - wireless to wired, fiber to copper. Each type has advantages and disadvantages.

Wired technologies

Twisted Pair - twisted pair is the cheapest and possibly the easiest type of media to work with. Over the years, we have seen the development of higher grades of cable - both shielded (STP) and unshielded twisted pair (UTP) that can handle higher-speed traffic. UTP is connected to devices using simple RJ45 connectors. Every cable will be affected by attenuation - the loss of signal quality over time. With analog communications, an amplifier was used to boost the strength of the signal and allow it to be carried long distances. With digital communications, a repeater that will regenerate the signal is used. Regenerating the signal also serves to reduce noise and improve the integrity of the data. Twisting the pairs of wires also breaks up the problem of crosstalk, where the signal from one wire may bleed onto on the wires that are nearby.

Coaxial cable - coax is generally better than twisted pair in capacity and distance, but it is more expensive, harder to work with, and not as commonly used. Coax consists of two conductors separated by an insulator and has excellent bandwidth. Coax cable is generally connected using BNC connectors.

Fiber Optic cable - the development of fiber optic cable led to tremendous improvements in bandwidth and quality of network communications. Fiber can handle traffic volumes far exceeding any other technology. Fiber, though, is more expensive, more difficult to work with, and less compatible with some devices. Fiber is, however, immune to some of the problems of UTP, such as radio frequency interference (RFI) and electromagnetic interference (EMI).

Wireless Technologies

802.11 WLAN - the 802.11 standards (and standards in development) for wireless local area networks are excellent for connecting devices in a defined area. Wireless routers enable wireless communications and also serve as an interface to wired networks. These are the most popular wireless standards in use. Several more are in development.

- 802.11a - this standard operates in the 5 GHz band at speeds up to 54 mb/s.
- 802.11b - this standard operates in the 2.4 GHz band at speeds up to 11 mb/s
- 802.11g - this standard operates in the 2.4 GHz band at speeds up to 54 mb/s
- 802.11n - this standard introduced the concept of Multiple Input/ Multiple Output (MIMO) in the 2.4 GHz band with speeds up to 600 mb/s
- 802.11ac - this standard operates in both the 2.4 GHz band at speeds up to 450 mb/s and the 5 GHz band at speeds up to 1300mb/s

802.15 - Bluetooth - short-range (10 meters/30 feet) communications between paired devices.

802.16 - WiMax - wireless metropolitan area networks that permit wireless access between cells within a metropolitan area.

RFID - radio frequency identifier is a short-range wireless communications technology that can be used to track items implanted with RFID chips, often used in inventory management and passports.

Optical wireless - technology based on optical communications using a laser between two locations with a clear line of sight. Very good speeds without the requirement for licensing fees that are required with a microwave.

Microwave - a line of sight communications technology that is based on a microwave radio frequency signal between two devices, used in campus area networks and long haul radio communications.

Satellite - radio frequency communications used for long haul communications often to areas not accessible through fiber or conventional communications media. Requires line of sight. Since the signal of a satellite can be picked up over a large area, it requires the use of encryption for sensitive data.

Mobile phone/cellular technology - data and voice communications across large areas by connecting to a 'cell' tower. Not line of sight. Variable speeds according to protocols and technology in use.

Network Layouts

Bus

The physical and logical structure of networks can also vary. The oldest networks were peer-to-peer networks (for example, a bus.) A bus is a network model where all the devices on the network are connected to a single communications path. This can be done using a cross-connect cable for two devices or a hub for more devices. This was also done with some of the older mainframe models. Each device on a bus type network is a peer - equal. If any device wants to communicate, then it puts its data on the bus network with an address of the intended recipient. As the data traverses the network, it is picked up by each device on the network. Each device checks to see if the data is addressed to it. If the address of the data is for a different device, then that device will just ignore the data. If two devices are sending a large amount of data, then this may impact the availability of the data for other devices since it is a shared network. This also means that the network is subject monitoring since a person can set their network interface card (NIC) into promiscuous mode and capture all of the traffic on the network.

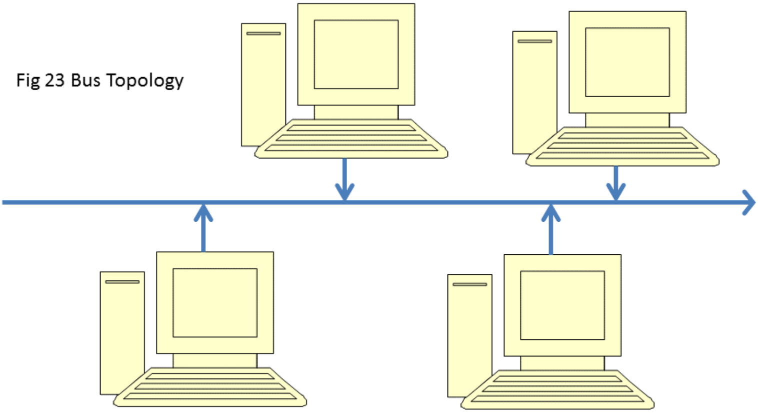


Fig 23 Bus Topology

Star Network Layout

The star is probably the most common network layout in use today, especially for local area networks. With a star, each device on the network is connected to a port on a central point, such as a switch. The switch can send traffic that is going from a device on one port to a device connected to another port directly and not send the data to every other port. This means that the traffic on a switch is a bit harder to monitor unless you have direct access to the switch. This can also have the advantage that a lot of traffic between two parties will not have, and as much impact on the other devices as would happen on a bus type network.

The advantages of a star network include the flexibility and ease of administration when all devices can be accessed from a single location. These networks tend to operate quite quickly, and it is easy to connect and disconnect devices or change their configuration. However, the disadvantages are cost and the fact that the switch and server room may be single points of failure if something happens to the switch, or there is a problem in the wiring closet or server room, everything can be compromised.

Virtual Local Area Networks (VLANs)

A switched network may also be divided into a set of smaller networks through the use of a VLAN. A VLAN separates the traffic from some ports on a switch from the traffic for other ports on the same switch. In this way, the switch is logically managing the traffic to the various devices on its ports as if they were on several different physical networks.

A VLAN may also provide logical management of traffic on several different switches so that devices connected to one switch may be treated as if they were on the same physical network being managed by another switch.

Fig 24 Star Topology

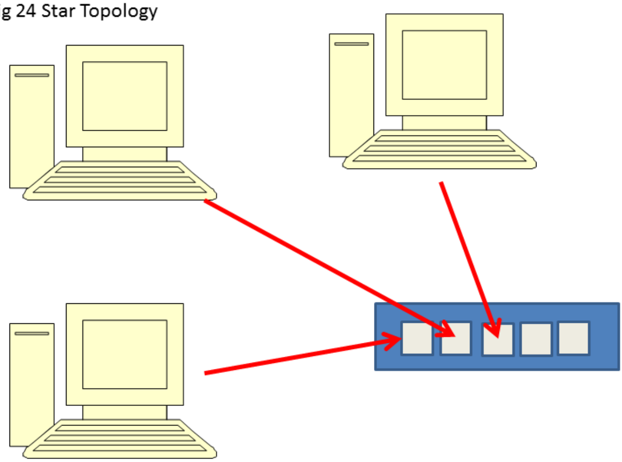
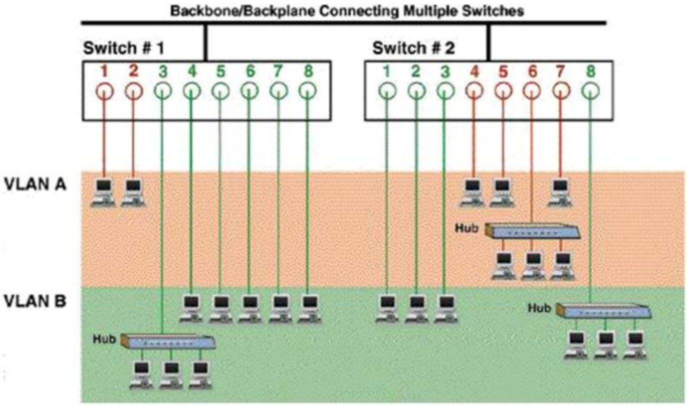


Fig 25 VLAN



Address Resolution Protocol (ARP), DHCP, and Network Address Translation (NAT)

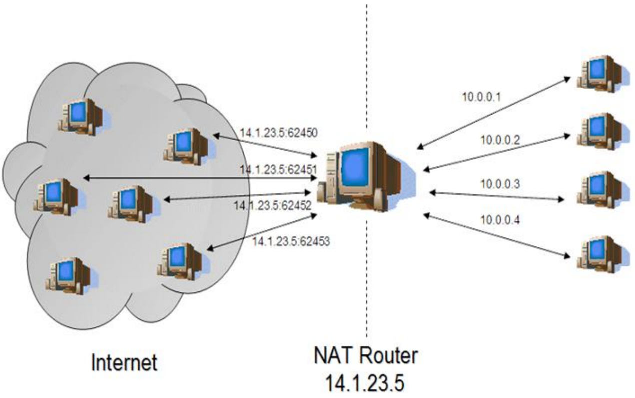
Many local area networks use the media access control (MAC) address of the network interface card on a device for addressing. When a computer is attached to a network, the physical connection is via the NIC card. The MAC address is a 48-bit address based on the manufacturer and the serial number of the card (its physical address). When the device first connects to a DHCP (dynamic host configuration protocol) enabled network, it is assigned a 32 IP address (its logical address). The DHCP server responds to a DHCP request from the newly connected device and offers (DHCPOFFER) an IP address to the newly connected device from its range of available IP addresses. The IP address is assigned (or leased) to the device for a set time.

Quite often, the IP address provided is based on the addresses currently used for internal addresses - known as the non-routable addresses - in RFC 1918.

RFC 1918 lists four addresses spaces that are non-routable and are most often used for internal addressing:
The entire 10.x.x.x network (where x is any value from 0 - 255)
The range of 172.16.x.x to 172.31.x.x
The 192.168.x.x network

This process is known as Network Address Translation (NAT). The internal addresses used on the network are for internal use only and could not be routed over the internet. This is similar to having an internal mail address for an office tower. Each cubicle or desk has an internal address (often comprised of the floor in the building and area on the floor). The mail to the company comes to an external address - perhaps a box number or street address. A clerk in the mailroom then sorts the mail and routes it to the internal addresses. A NAT firewall does the same thing. When traffic is going out from the internal network, the firewall changes the source address (the address of the person going out of the network) to the external address of the firewall. This allows the remote device that the user wants to talk to, to be able to reply by sending its reply to the external address of the firewall. The firewall then converts the destination address of the reply to the internal address of the party that requested the information.

Fig 26 Network Address Translation



For the switch to route IP-based data to the device on the correct port, the switch must know which IP address has been assigned to the device. The switch creates a cross-reference table that lists the IP addresses and their associated MAC addresses using Address Resolution Protocol. ARP requests are broadcast by the switch to the entire network; it manages to ask who is currently associated with an IP address. The device that has been leased or assigned that IP address will then reply by identifying its MAC address. The switch keeps that in a table (cache) so that any future traffic to that IP address can be routed to the correct device.

ARP messages are unauthenticated, which can lead to data compromise. A malicious person may send a reply to an ARP broadcast, or even an unsolicited reply to the switch identifying themselves and their MAC address as the owner of an IP address. If the switch accepts that information, it will begin passing the information to the MAC address of the malicious person as well as, or instead of sending it to the correct owner. This would allow the malicious individual to monitor all traffic meant for another person.

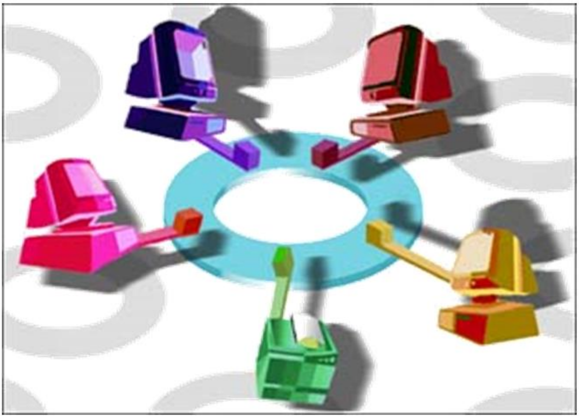
Tree Network

A star network can be quite large but will often be integrated into an even larger network as a part of a tree network. With the use of trees, a network is very scalable and can become quite large. A breakage in the connection between the various branches of the tree could cause a loss of communications, but that may be addressed through the use of a redundant route.

Ring Networks

A ring network connects all the devices on a network in one ring. This network configuration is rarely used today for local area networks but is still used a lot for internet backbones where a high level of throughput and reliability is required. The use of dual rings can provide failover capability through redundancy.

Fig 27 Ring Diagram



__Mesh and Partial Mesh Networks__

The internet is a partial mesh network. It was designed to be tolerant to the loss of a portion of the network so that even if a major city or region that lay in the middle of the network was cut off, communications would still be possible through other routes. This fault tolerance is possible because many of the primary internet systems are linked to several other systems through multiple links. The failure of one node or portion of the network will affect traffic in that location, but the rest of the network will still be able to communicate.

A full mesh network would require every device on a network to be connected to every other device. That would ensure that the loss of any one device would not affect

Network Communications Control

Managing a network that supports many devices requires some form of communication control so that the devices can communicate effectively even if every device wants to communicate at the same time. There are several methods of controlling network communications in use today.

For most organizations, the network, or carrier, of the traffic must provide reliable and accurate communications. There must be a way to ensure that the correct traffic, without alteration, is sent to the correct party. Also, some networks may require encryption for the confidentiality of the data being transmitted. The first step in network communications is to support the type of network media involved. The communications requirements are substantially different if the network media is fiber than if the media is satellite or copper. The size and format of the packets may be quite different. There is also a wide difference between communications over a dedicated link such as T1 or E1, as compared to communications over an on-demand connection such as a fax machine.

If a dedicated link is to receive many millions of bits of information per second, the end devices must be able to separate each individual block of data from the other blocks around it. In other words, they must be able to separate each byte or character from the other bytes. This becomes especially challenging when the network is multiplexing many channels together into one data stream. For example, with a T1 line, 24 channels or individual communications can be transmitted through the network at once, at a speed of 1.544 megabits per second. The receiving end must be able to demultiplex the traffic back into individual channels, while a clocking signal is used to maintain the correct timing of the two endpoints so that they can combine and separate the channels correctly. This is an example of synchronous communications.

A fax machine is an example of asynchronous communications. A fax machine sets up a connection on demand - when required, and when the two devices initially begin to communicate, they have to determine the best speed to use. Some machines will have the ability to operate at higher speeds than others, and sometimes the network will only permit a certain speed. Once the speed has been established, the data itself will be sent as individual pieces, often as individual characters, and each character will be wrapped with a start and stop bits to signal the start and end of each character (each piece of data).

Carrier Sense Multiple Access with Collision Detection (CSMA-CD)

When several devices are sharing the same communications media (or carrier), it is necessary to manage the traffic so that the data transmission from one device does not disrupt the data being sent by other devices. There are several ways to manage network communications. The first of these is through carrier sense - or, in other words, the ability to sense or listen to traffic on the carrier medium. When a device wants to transmit data, it listens first to see if the network is already in use. If it is not, it may be transmitting its data. While it is transmitting, the device continues to monitor the network. If it detects a collision with other data, it will cease to transmit and wait before trying to resume its transmission until the network is once again clear.

This process of managing traffic is used by Ethernet and other communications processes that can both transmit and receive at the same time. It is fairly efficient in that it does not require extensive overhead to manage traffic. However, it suffers from a lack of efficiency when traffic volumes are high since every time a device wants to communicate its results in a collision and poor network performance.

Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

Not all communications support full-duplex communications where the sender can both transmit and receive at the same time. For example, most radio transmissions will not allow a person to hear while they are speaking. This means that a sender will not know if someone else is transmitting at the same time. To manage communications in such circumstances, CSMA-CA is used. In this case, a party that wishes to transmit will signal to the destination and request to send (RTS). The destination will then respond with a clear to send a reply (CTS). All the other devices on the network will then know that a communications decision has been made and will not transmit until the network is clear. The two devices that have agreed to transmit will communicate and often provide acknowledgments to each other to validate successful transmission.

Polling

Polling is used by networks that require high integrity communications. To ensure that all devices are online and able to respond, a master device manages all communications and sends a note to each device on the network, in turn, asking if they have data to transmit. A device will respond, thereby validating that it is online and providing any information it has to send. Still, it will only communicate when it is polled by the master device. This form of communication is frequently used in networks that handle alarm circuits and video lottery terminals or other areas requiring carefully controlled communications.

Token Passing

Token ring networks operate on a deterministic communications process and use a token to control data communications. The token circulates around the ring at a fixed speed, and a device is only able to speak when it has possession of an unused token. Since the token circulates at a fixed speed, each device knows that it will have the ability to communicate at regular intervals.

Network Devices

Many types of devices make up networks of today. Several devices have faded away and no longer in common use.

To transmit long distances, it is often necessary to install devices such as repeaters that will compensate for the attenuation of the signal.

Switches

Several terms used in network communications are quite broad and can have several different meanings. Some examples of this are the terms switches, firewalls, and VPNs. There are many types of switches with various functions, just as there are several generations of firewalls, many of which are considerably different in their function and operation.

Switches are used to connect devices together, and switches today perform the functions formerly provided by hubs and bridges (layer two). Switches forward packets to a destination, can perform routing functions (a layer three switch), address translation and balancing (layer four), and do load balancing (a layer seven switch).

Switches can be used to connect networks but also segment and divide networks through configurations such as a VLAN (Virtual LAN) where different devices physically connected onto one switch may be set up to act as completely separate networks.

Switches can be wired or wireless, small and inexpensive, or large and very expensive. Each organization must determine what equipment is suitable to meet its network requirements.

Routers

The purpose of a router is to connect multiple networks together and forward incoming packets as best it can in the direction of the destination IP address that is in the packet header. A router can vary in size from a wireless router in a home that connects the computers in the home to the internet, to large core routers that are responsible for the routing of high-speed internet communications. The router builds a routing table using routing protocols such as Border Gateway Protocol (the first routers were called gateways) and learns how best to direct traffic towards its destination. In many ways, a router is like a traffic circle used to handle vehicular traffic. Traffic enters the circle and then routes off on the road that is best towards the ultimate destination. The intelligence of the routing decision is similar to the decision made by a driver - to take the shortest route, the fastest route, the route with least construction delays, etc. So also, a router may direct traffic over different routes depending on traffic volumes and congestion.

Just like on the road, some traffic has labels that indicate it has a priority, similar to emergency vehicles that are permitted to bypass other traffic that is waiting to be routed. The label, like the siren on an emergency vehicle, indicates that this packet should be processed quickly and not be held back, waiting for other packets to be processed. The delay in processing is called latency, and this would severely affect the quality of some types of traffic, such as Voice over IP (VoIP). The labeling of the traffic allows for the provision of Quality of Service (QoS) and Class of Service (CoS) traffic management. QoS is usually used to provide guaranteed bandwidth for traffic volumes, and CoS is used to grant priority to certain packets over others (for example, voice packets over regular data packets). This also prevents the jitter that would affect data traffic from impacting voice communications. Jitter is the variation in the arrival time of a packet due to different routing, latency, etc.

Firewalls

The simplest definition of a firewall is a mechanism that protects one network from another. As a security manager, it is important to remember that firewalls should be used to control both incoming and outgoing traffic. The term firewall refers to many types of technology that operate at various layers of the OSI model and have evolved significantly over the past years. The most basic and first-generation firewall is the simple packet filtering router that examines individual packets and enforces rules based on addresses, protocols, and ports.

Second-generation firewalls would keep track of all connections in a state table. This would allow them to enforce rules based on packets in **the** context of the communications session.

Third generation firewalls operate at layer seven (the application layer) and can examine the actual protocol being used for communications - for example, HTTP. These firewalls are much more sensitive to suspicious activity related to the content of the message itself, not just the address information.

Next-generation firewalls - sometimes called deep packet inspection are an enhancement to third-generation firewalls. They bring in the functionality of an IPS (Intrusion Prevention System) and will often inspect SSL or SSH connections.

It is important to ensure that the firewall configurations are backed up regularly and reviewed to ensure that all rules are in the correct order, are documented, and that the firewall is tested on a scheduled basis.

Of course, a firewall is only as good as the person that manages it, so an important role of the security manager is to verify that the staff managing the firewalls and other network devices are knowledgeable, trained, and supervised. Firewall logs must be reviewed regularly to detect any suspicious activity.

Proxy

A proxy is a device that acts as an intermediary between two communicating parties. The proxy acts to the party on each side of the communication as if it was the other end host. This allows it to filter and examine suspicions activity, protect internal resources, and take action if an unacceptable activity is occurring. A gateway is often a type of proxy that controls traffic through a gate or security perimeter.

DNS

For most people, the DNS (domain name system) is the mechanism that makes the internetwork. Without the DNS, they could not navigate to their destination website without knowing the IP (internet protocol) address of the website they wanted to visit. The DNS provides a simple cross-reference that is used to associate a “normal” name with the IP address used by network devices. The IP address is a logical address given to a website based on the addresses allocated to the ISP (Internet Service Provider). Individuals can purchase a name for their website that is more in line with their name, the name of their organization, or their marketing program. The IP address for Mile2.com, for example, is 206.214.216.216. A person wanting to visit the Mile2 website could simply type in *http://206.214.216.216/*. That is the “real” address of the website. However, it is much easier to remember and enter *www.mile2.com* than it is to remember the IPv4 address. DNS is a tree structure that resolves the addresses so that a network device that receives a request from a person entering *www.mile2.com* will be able to look up the IPv4 address and then route the request properly through the network. When a network device does not know the IP address associated with a 'web name,' it sends a DNS request up through the DNS tree to a higher level DNS resolver; the reply is then sent to the requesting device using UDP over port 53. The requesting device will then store the IP address and name for future use.

There have been many attacks on the Internet using DNS; People have sent false DNS replies that would misroute traffic, and DNS replies have been used in amplification attacks to flood a victim's system. People have done 'cybersquatting' to reserve the names of sites that another organization may want and only agree to sell that name to the organization at a higher price. DNS can sometimes be used to 'learn' information about a company and its administrators that can be used in attacks.

Network Defense

Network defense is an excellent example of the use of layered defense. Networks security starts with protection at the perimeter of the network using firewalls and network segmentation. The area of the network that is accessible to outsiders on the network is isolated into a demilitarized zone (DMZ). This prevents an attacker from having direct access to internal systems; all devices in the DMZ are hardened with all unnecessary functionality disabled. Such devices are often referred to as a Bastion Host. In the DMZ and at other points on

the network are IDS (intrusion detection systems) and IPS (intrusion prevention systems) that monitor record and may block suspicious activity. The application firewall in the DMZ is behind a packet-filtering router to clear out most of the bad traffic before it gets to the application firewall.
Inside on the network is more segmentation between various departments and systems to restrict traffic from areas it does not need to access.

Each device connected to the network is also secured with antivirus, a firewall, and Host-based IPS.
The above is an example of a layered network defense.

Encryption of Network Traffic

There are several ways to encrypt network traffic depending on the layer in the OSI stack, where the encryption is to be done. In many cases, data may be encrypted more than once. For example, an encrypted email sent over a wireless connection will be encrypted at the application layer (email) and again at the data link layer (WPA2).

Datalink layer encryption

The lowest level of encryption is at the data link layer. This encrypts the data between two adjacent devices. An example of this is to use WPA2 to encrypt data between a laptop and the wireless access point- a link-layer encryption. The problem with link-layer encryption is that the data must be decrypted at each end of the link, and if the data is going to transmit across another link, then the data must be re-encrypted. An example of this problem is when an organization is using handheld wireless payment devices. For most devices, the data is encrypted over the wireless link and then decrypted at the wireless gateway before being re-encrypted to transmit over the internet to the bank. If a person taps into the wireless access point, then they can capture the payment card data at that moment that it is unencrypted.

Network Layer Encryption

Encryption at the network layer is done using IPsec (Internet Protocol Security). IPsec has several modes of operation that can be used; Authentication Header (AH) and Encapsulating Security Payload (ESP). Each mode has a different function.

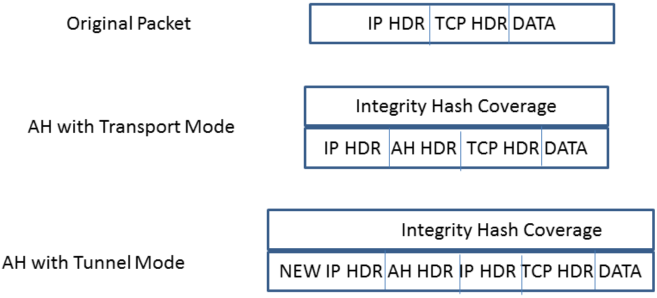
Authentication Header is used to do what its name says - authenticate the IP header information. In the IP header are several fields, including the source and destination addresses, and a checksum that is used for integrity.

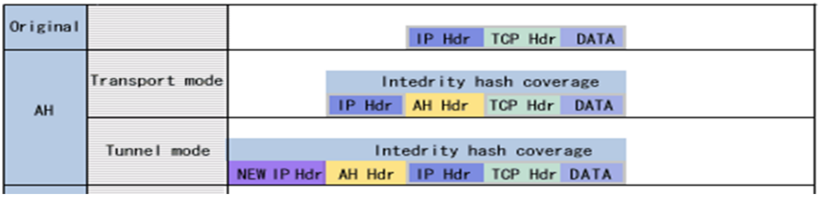
IPSEC is designed to ensure the integrity and authentication of two parties that are communicating over the internet - a connectionless communications process. How can we know whom we are talking to (preventing masquerading, man-in-the-middle, or spoofing) and know that our communications have not been altered en route? This is what AH can do for us.

The first step in establishing an IPsec tunnel is using IKE (internet key exchange) to exchange a SA (security association) via Oakley and ISAKMP (Internet Security Association Key Management Protocol). Oakley is an implementation of the Diffie-Hellman key agreement protocol and sets up the encryption keys to be used. The SA is used in IPsec to validate the identity of the originating party. The SA contains the source address and mode of IPsec to be used and a security parameter index, which provides a unique identifier for the communications session. A SA must be sent from each party to the other since it authenticates the source.

When using AH, a new IPsec Authentication Header is inserted into the packet after the IP header. The benefit of AH is that it verifies the authenticity of the sender and the integrity of the packet.

Fig 28 IPSEC AH





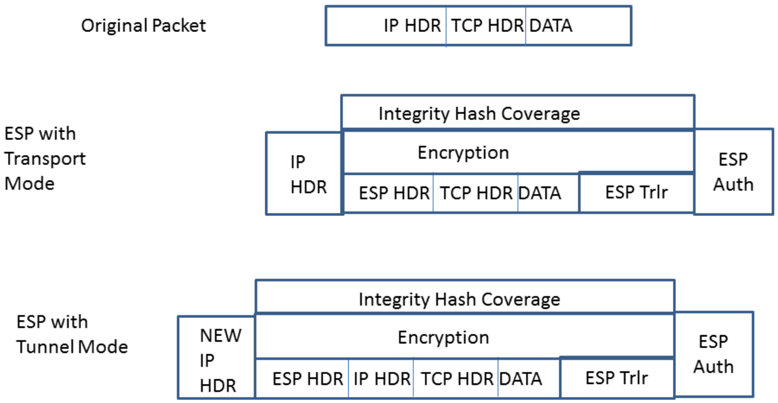
Also, when data confidentiality is required, IPsec can be used in ESP mode. ESP provides the same benefits as AH and adds in encryption of the data being transmitted.

There are two modes of ESP that are used - Transport mode and Tunnel mode.

In transport mode, a new ESP header is inserted between the original IP header and the transport layer header. The ESP header provides for authentication and integrity, just like AH, but the data in the packet is also encrypted, providing data confidentiality.

In tunnel mode, a new IP header is created. This header is based on the IP addresses of the two ends of the IPsec tunnel. Most times, IPsec is used from network to network instead of between two end-user devices. This means that the ends of the IPsec tunnel are at a firewall or VPN concentrator instead of at the end-user device. The original IP header is encrypted along with the rest of the packet - this provides authentication, integrity, confidentiality, and also helps hide the identity of the true sender and receiver of the message.

Fig 29 IPSEC ESP



Transport Layer Encryption

The protection of data at the transport layer is done using SSL (Secure Socket Layer) or TLS (Transport Layer Security). TLS was based on an earlier version of SSL.

SSL is used to create a secure tunnel from a client to a web server - often for e-commerce and other secure transactions. In most cases today, SSL is used as reverse authentication. Simply put, the webserver responds to a request from a client by proving to the client that the client is at the correct web server. For example, when a client logs in to a bank's website, the bank sends a certificate to the client that authenticates the identity of the webserver. The certificate also contains the public key of the bank. The client can use this public key to encrypt a session (symmetric) key and send that to the bank. The session key can now be used by both the bank and the client to encrypt the banking data they are sharing. This is an example of the use of asymmetric cryptography (for key management) to enable the use of symmetric key cryptography (fast, confidentiality) for data communications.

In the future, we may see the use of mutual authentication for TLS. This means that in addition to the bank sending a certificate to the client to prove their identity, the client would also have to send a certificate to the bank, proving who they are.

SSH2

SSH (Secure Shell) and its successor SSH2 provide an encrypted channel (tunnel) for logging into another computer over a network, executing commands on a remote computer, and moving files from one computer to another. SSH provides strong host-to-host and user authentication as well as secure encrypted communications over the Internet.

Virtual Private Networks (VPNs)

It was once eloquently written that a VPN was designed to "carve a tunnel through the internet." The internet is an insecure place, and it is rather simple to listen in on traffic passing over the internet or other connections such as wireless, satellite, or microwave. The use of a VPN to create a tunnel for the exclusive use of the two endpoints is a wise decision. Though , it should be pointed out that not all tunnels are encrypted. Layer 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP), and Point to Point Tunneling Protocol (PPTP) do not provide encryption. Using L2TP for remote administration (SNMP - simple network management protocol) or other such services requires that the L2TP traffic be routed over IPsec for confidentiality.

A VPN is a generic term, and all of the encryption and tunneling products listed above can be described as a VPN. The endpoints of a VPN tunnel should be located in a place that will allow the traffic passing over the VPN to be examined once it has been decrypted. Otherwise, malicious traffic traversing the VPN could circumvent firewalls or other network defenses.

Network Attacks

Networks are exposed to many attacks every moment. Some of these attacks are against the network itself, such as a denial of service, and some are against the devices connected to the network, such as a virus or logic bomb. The simplest attack on a network is often damaging the cable or network connection itself. Other attacks include sniffing the traffic on the network, jamming wireless signals, intercepting and modifying network traffic (often through a ‘man-in-the-middle’ attack), and misconfiguring network devices.

Denial of Service

Denial of service (DoS) attacks is a common method of attack and very simple to conduct. Many DoS attacks are used as a revenge attack against a company (or country, the case of Estonia that suffered a massive DDoS attack that lasted for several days), while others are used to hide other malicious activities. A denial of service attack aims at disabling the systems or operations of the target. There have been many ways to conduct network-based DoS attacks including the Ping of Death (a malformed ICMP ping packet), SMURF (a flood of ICMP packets), Fraggle (a flood of UDP packets), SYN floods (a flood of TCP SYN requests), and NTP (Network Time Protocol) floods, to name a few!

A DoS can also be against other systems or services - for example, an organization that is subject to a strike by their staff will often find it difficult for other workers or customers to gain access to the building.

A DDoS or Distributed Denial of Service attack is a denial of service attack launched from many points at once against a target. The use of many systems to attack a target amplifies the attack and can be difficult to defend against.

Botnets

Botnets, or robotically-controlled networks, are one of the largest problems on the internet today. A botnet is a collection of compromised devices that have been infected with a program that allows them to be accessed and manipulated remotely. The infection may be through a ‘zombie’ that sits on a victim’s machine and listens on an Internet Relay Chat (IRC) channel or through a program such as Zeus (also known as ZBOT) or Citadel that allows an attacker to read everything being done on the victim’s machine. ZBOT is often used in financial fraud, whereas many zombies are used in the distribution of spam or malicious content.

INCIDENT MANAGEMENT

The way an organization prepares for and handles incidents is one of the critical factors in the success of the organization. Incidents will happen despite the best precautions and preparation. If not addressed in an appropriate manner, the incident can lead to the collapse of the organization either financially or through damage to the reputation and confidence that customers, suppliers, and investors have in the sustainability and long term potential of the organization.

Events versus Incidents

An event is any measurable occurrence - a person logs in, a person logs out, a job completes. Most events are harmless and a part of normal business operations. However, some events have the potential to disrupt business operations. Such events are incidents. An incident should be recorded, managed, and resolved as quickly and effectively as possible to minimize the potential or real damage. This requires an incident management program that is focused on the steps needed to detect, escalate, respond to, and recover from an incident through trained staff, clear procedures, reporting, and accountability.

In the past, the term 'crisis' was often used instead of 'incident.' Because of the negative connotation of the term crisis, many organizations tend to use the expression incident now as in incident management instead of crisis management.

Priorities for Incident Management

The priorities for incident management, according to ISO27002:2005, are:

- Communications to allow for the timely intervention
- Quick effective and orderly response
- Documentation and audit trails
- Action to recover from and control the incident
- Feedback and learning from the incident

Steps to Incident Management

NIST defines the steps of an incident response plan in Special Publication 800-61 as:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-incident Activity

However, most incidents are not linear. It is not a simple, straightforward process from one step to the next. Many incidents will require several iterations of the second (detection) and third (containment, eradication, and recovery) steps.

Each incident is an opportunity to learn. Improvements can be made that will;

- help reduce the likelihood or impact of a future event,
- improve the detection and response capability of the organization,
- highlights areas for additional training, and
- potentially improve processes or business operations that were subject to failure.

Preparation

Effective incident management starts long before the incident ever happens. Preparation is often the key to success, and preparation, in this case, means to make as many decisions, and take as many steps as possible to be ready for an incident. Few people make right decisions under pressure, so a key part of preparation is to make as many decisions about responsibility, response, or network isolation.

The preparation and development of the incident response plan will also consider input from risk assessments and business impact analysis efforts to ensure that critical assets, systems, and processes are identified, risks are addressed, and the plan is aligned with the priorities of the organization.

Unfortunately, some incidents can be severe and may require the involvement of external parties such as law enforcement and regulatory agencies. Incident management requires that the conditions and steps to be taken to interface with these external parties are defined in advance, and there must be an appointed liaison that will be the organization's representative to work with these parties.

This also requires that the legal counsel of the organization and human resources departments are included in the incident response plan and team. When employees are represented by a union, it can be advisable to work with the union as well to prepare for how to deal with contract terms and working conditions during a crisis.

Any incident that involves a publicly known situation also has the potential complications of media involvement. This requires

the preparation of the public relations department to be ready to face public scrutiny and attention.
Some incidents will require team members with specialized skills - forensics, financial audit, IT. The preparation of the incident management team should identify those required skills and ensure that the staff is trained and ready to deal with an incident once it happens. This often includes the development of a 'battle box' that contains all of the equipment and supporting items that may be required when responding to an incident. If the team is alerted of a potential incident, all that has to be done to mobilize the team is to grab the battle box and go. They do not need to frantically look around for the items they would need at the time of the crisis.

Items in a battle box may include:

- Radio and portable communications devices
- Flashlights and batteries
- Documentation and blank forms
- Pens, markers
- Evidence bags and labels
- Spare drives
- Write protect cabling
- Hand tools (screwdrivers, wrenches)
- Camera
- Gloves
- First aid kit

Writing a Plan

A plan must be legal, authoritative, clear, unambiguous, action-orientated, and available. The team members must know the plan, and the organization, especially senior management, must have confidence in the plan so that it can be carried out in a crisis. An incident is not an excuse to break the law, and every organization must know the laws and regulations that apply. There are labor laws, environmental laws (dumping of hazardous waste), health and safety laws, privacy laws, criminal laws, or civil liabilities must all be known.

The plan should not be excessively wordy, but rather contain short action-orientated statements and clear directions. The use of checklists in the plan can help track what has been done, what still needs to be done, and ensure that no critical step is missed in the heat and pressure of the incident.

Responsibility

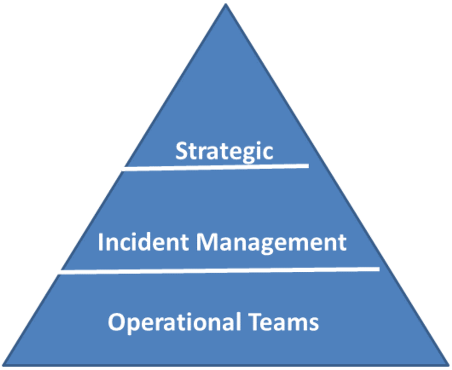
During a crisis, one of the most damaging problems can be a lack of authority or leadership. Not everyone is a good leader in a crisis, some people do not do well under the pressures and uncertainties that accompany a crisis, and they are unsuitable to be the leader. Other people do well under pressure; they can make right decisions, exude confidence and positive morale, and bring calm professionalism to the crisis. Such people need to be identified and placed in positions of crisis leadership. Everyone should know who the leader is (and in the absence of the normal leader, who the deputy is as well), and all communications should be conducted to the proper channels and leaders. Even during a crisis, the organization should be thinking strategically - where is the organization headed? What changes will this incident make in the culture, operations, and processes of the organization? If we have to rebuild, how can we rebuild with a vision to the future and understand how to use this incident as an opportunity to improve?

The overall strategic leader must be a person that can delegate responsibility to trustworthy team leaders. There may be many separate initiatives going on simultaneously, and each initiative should have a leader that can handle their area of responsibility with little oversight and report on the status of their responsibilities back to the overall leader.

Therefore, to manage the incident, the organization may have three levels of teams.

- The strategic team governs and provides oversight and direction for the incident. It must also deal with the legal, public relations, and customer and employee communications issues.
- The incident management team provides oversight for the various operational teams and directs the recovery operations. They also feed the status report to the strategic team.
- The operational teams are doing the various actions and steps necessary to recover individual operations, departments, or business functions. These skilled people implement the steps of the plan and rebuild business operations.

Fig 30 Incident Management Triangle



Policy

The first step to incident response needs to be the development of an incident response policy that outlines management's commitment to protecting the assets of the organization and responding to incidents in a legal, responsible manner. The policy also gives authority to the incident response team for assuming a leadership role and implementing the response plan during the incident.

Budget

The budget for an incident response should include a sufficient budget for writing the plan, training the incident response team members, testing the plan, maintaining the plan, and purchasing the equipment needed to prevent, detect, respond to, and recover from incidents.

Detection and Analysis

It has been said that "Some people make things happen, some people watch things happen, but most people wonder, 'what happened?'". This is all too true in incident management. From the 2011 Verizon data breach report, we see that nearly 2/3 of all organizations that suffered a data breach were not even aware of it and had to be informed of the breach by a third party. This is a serious problem that hinders effective incident management. An organization cannot respond if it is not even aware of what happened.

Detection Methods

A report is only valuable if somebody reads it, and that is truer than ever today. Every day, organizations gather massive amounts of log data and spend incredible amounts of money on Security Incident and Event Management (SIEM or SEIM) systems. They also spend on other alert and monitoring systems that capture network, application, and user data. However, in far too many cases, it can be noticed that no one has the time or responsibility to monitor the logs. Intrusion Detection Systems will not really protect an organization; all they do is indicate the types of incidents that happen. Sure, they can work with other devices to drop connections or alert about suspicious activity. Still, they are only as good as their configuration and only as effective as the staff that leverages the data collected.

Knowing normal activity levels will also assist in being able to detect any types of abnormal activity.

Audit logs are important and should record all activity on a system or at least activities that are sensitive or critical, such as administrative changes or incidents where a person viewed protected data or tried to log in with the incorrect information. Synchronizing data between various logs requires the time on each device to be synchronized - otherwise, it can be very challenging to associate activity between the logs.
Other detective devices are firewalls, host-based intrusion detection and prevention systems, and application logs. Each tool can assist the organization is tracking types and frequency of attacks, the misuse of the system by users or administrators, and frequent errors or misconfigurations. The organization should conduct vulnerability assessments and penetration tests regularly to help identify any weaknesses or gaps in their security.

People are the best incident detection device for an organization. Everyone within the organization should understand their responsibility to watch for and report any suspicious activity. Outside people may also be a source of information about possible incidents. The organization should have a process for an outsider to report a problem if a potential problem is detected.

Classification of an Incident

Once an incident has been detected, the first step is learning the scope, size, and potential impact of the incident. An incident poses an immediate risk to the organization, but also may pose a long-term risk as the effect of the risk may ripple out to other areas, downstream operations, or business partners. Incidents can be classified according to their location (geography), impact on business operations (departments, enterprise-wide), financial cost, impact on health and safety (always the priority), and reputation.

The classification of an incident is often based on whether the incident is internal or external, whether it is accidental or intentional. The classification of the incident will drive the response strategy.

Notification

When an incident has been detected and classified, the next step is to notify the appropriate stakeholders. The stakeholders include senior management, affected departmental managers, regulators, law enforcement, legal, human resources, security, public affairs, and system owners. Depending on the type of incident, stakeholders may be notified by email, phone calls, in-person, or websites.

Mobilization of Incident Response Teams

When an incident occurs, the appropriate team members need to be notified and assembled as rapidly as possible. Depending on the type of incident, not all team members may need to be activated - unneeded team members should not be activated to expending unnecessary resources.
The plan must contain current contact numbers and procedures for each team member. A common method of mobilizing the team is through a call tree where the leader will call the first tier

of responders, and then those people will call the next tier and so on.

Containment

Containment prevents the expansion and increase in damage caused by the incident. The containment strategy attempts to respond quickly to an incident and ensure that the incident will affect as few departments, networks, people, and systems as possible while minimizing the financial and reputational cost.
A common containment strategy is to isolate affected systems or networks. This requires preparation to know which systems can be isolated, what the impact of the isolation would be on other systems or business operations, and how to isolate a system effectively.

The primary goal of the organization is usually to recover as quickly as possible and get back up and running with minimal impact, but this may be difficult where the incident involves law enforcement or other investigators. Their objective is to gather evidence, and the recovery of systems may damage evidence that may be needed for further investigation.

A challenge with any incident is the breakdown of normal controls. In normal circumstances, there is a separation of duties and precautions to protect sensitive information or protect against unauthorized changes. However, in a crisis, many of those controls may be removed. Administrators may be able to make changes without peer review, external parties may be accessing the facility, and confidential documents may be exposed. This increases the need for appropriate security controls to be in place immediately following a disaster.

Communications

When reviewing past incidents, one common theme is addressed in the documentation, and that is the challenge of communications. Incidents breed rumors and suspicion, and the only way to combat the negative impact and uncertainty associated with the incident is through effective and timely communication.

The organization should have plans in place to communicate with employees, customers, suppliers, and the general public. Communications should be handled by authorized personnel that has been trained in how to handle the media. In a world of social media, the organization must be diligent in communicating promptly and honestly through all the common channels of communication in use today - website, social media, print, radio, and television.

Evidence

Evidence is the material data and artifacts that can be used during the investigation of an incident. Any evidence that could be used in the investigation should be identified and then collected according to approved practices and procedures. All evidence should be collected so that the evidence is complete. Evidence must be gathered legally and in a way that preserves the integrity of the evidence (it has not been altered inappropriately). The gathering of evidence starts the chain of custody of the evidence. The chain of custody is an unbroken documented record of all actions to, ownership of, and location of the evidence at all times from its initial seizure until it has been released (destroyed or returned to its owner).

If the chain of custody has not been preserved for the evidence, or the evidence has been altered in any improper manner, the evidence may not be trusted or admissible in the investigation. First-hand evidence that has been collected by the investigator is always preferable to secondary evidence such as copies of evidence or oral reports. Evidence that cannot be directly verified by the investigator may be rejected as hearsay. The incident manager should keep a record of any identifiable attack vectors (IP addresses, user accounts) that were used in the attack.

Some evidence - such as advanced digital forensics may require the expertise of an outside agency to process, analyze, and report on the evidence. When dealing with external agencies, care must be taken to protect the privacy of data, the standards for reporting the data, and the handling and transportation of evidence. Provisions must also be in place for how to handle the situation if criminal activity is found during the evidence processing activity.

Eradication and Recovery

Eradication is the removal of the incident - such as in the case of a virus, the removal of the virus. Any damage done by the incident should be corrected, including backdoors or fake accounts set up by an attacker. Any vulnerability that allowed the attack to succeed should be patched, and the system returned to normal operations. Afterward, the system should be tested for any other weaknesses before being restored to operation.

An attack on an information system may require the complete rebuilding of the system from a backup since many rootkits and other types of malware can be nearly impossible to eradicate.

Integration with Business Continuity and Disaster Recovery Plans

Many incidents can be handled using an incident management plan. However, when an incident would result in an outage or interruption of unacceptable length, the focus may shift to business continuity and disaster recovery plans. Business continuity plans are used to keep critical business products and services operational despite the crisis. This may require the move of operations to another location or outsourcing certain activities. Disaster recovery plans are concerned with the rebuilding of IT systems, networks, and operations. The incident management plan should be coordinated with the business continuity plans so that the business continuity teams can be activated and recovery efforts coordinated effectively.

As changes are made to the organization and the various plans, the plans should be reviewed and coordinated to ensure consistency or prioritization, timelines, staff, and responsibility.

Testing the Incident Response Plan

The best test for an incident response plan is an actual event, but obviously, it is best to test the plan before a real incident occurs. Various tests should be performed - such as an annual review just to make sure contact information is correct, and other data in the plan is up to date. As staff changes, the plan must also be updated, and new staff trained or brought into the response teams.

The plan should be reviewed by the incident response teams regularly, and the team may execute a tabletop exercise where they will step through the plan together as if they are responding to a real incident. Team members with specialized skills should practice their use of tools and ensure that they are prepared to deal with a real situation competently and professionally.

Feedback

Every incident is a learning opportunity. The organization must use the details of the incident to improve their processes, incident response capability, and train their team members. All team members and affected departments should be involved in the feedback process. The input of each participant should be encouraged, and efforts should be made to avoid finding blame or criticizing other participants. All lessons learned should be documented, and an action plan to address those items should be created.

Reassess Risk

An incident is the result of an unmitigated risk, and the incident management team needs to ensure that they have found the root cause of the incident, not just the symptoms. This analysis will lead to a reassessment of the risk and vulnerabilities of the organization and the evaluation of the effectiveness of the controls that are in place. Adjusting controls, patching and hardening systems, reviewing procedures, and planning for the implementation of new controls are all positive results of a risk assessment process.

Key Performance Indicators (KPIs)

When evaluating the effectiveness of the incident management plan, the organization may use key performance indicators to measure and track the effectiveness of the plan.
A key performance indicator allows the organization to compare the results of previous incidents with current performance. This will identify improvements that have been made and highlight areas that still need further improvement.

Common KPIs are related to:

- Time to identify an incident (detection capability)
- Time to mobilize response teams (reaction capability)
- Time to clear an incident (response capability)
- Progress in addressing issues found during feedback review.

Other areas of the review can relate to the performance of the incident response team members. This review measures the cooperation and coordination of the teams and team members. It also measures the assessment of the skills of the team, reporting and monitoring capabilities, the completeness of the plan and any missing elements, and the effectiveness of the feedback and review process.

Maintenance of the Incident Response Plans

The incident response plan must be maintained so that it can be used effectively when an incident occurs. This requires the review of the plan and the training of new team members. All key team members should have a succession plan so that another person can step into their role if they are unavailable. The plan should be updated with any changes and then distributed to all key team members. The plan must be available even if the core information systems of the organization are disabled. Therefore, paper copies of the plan should be retained offsite.

Summary of Incident Management Planning

The security manager should be prepared to deal with incidents that may occur. This requires processes to detect, respond, contain, analyze, eradicate, recover from, and learn from any incident. Plans should be written so that the organization is prepared, and the response team is ready.

APPENDIX A:

INFORMATION SECURITY PROFESSIONAL CERTIFICATIONS AND EXAMINATIONS

Many people that work in information security are interested in sitting for one of the examinations that lead to certification as an information security professional. This may be important for several reasons, such as the career opportunities that certification may provide, as well as meeting the requirements for certification that many organizations necessitate for a professional holding a job in this field.

There are several certifications sought by information security professionals. Each one is slightly different but based on the core concepts of information security that are documented in authoritative reference books. This appendix will look at the characteristics of each of the major certifications, the Certified Information Systems Security Officer (CISSO) from Mile2; the Certified Information Security Manager (CISM®) from ISACA®; and the Certified Information Systems Security Professional (CISSP®) from (ISC)2®. \

Each certifying body has its own set of requirements for certification, including codes of ethics, experience requirements, logistical criteria for examination registration, annual fees, and requirements to prove ongoing education and experience. These vary widely and are subject to change on an irregular basis, so it is always recommended that the certification candidate frequently checks with the certifying body to ensure that they have the latest information. The information provided here is accurate at the time of preparation but is not authoritative or necessarily accurate at any future time.

Certified Information Systems Security Officer (C)ISSO)

The C)ISSO certification was developed and maintained by Mile2 (*www.mile2.com*) in cooperation with several governments and militaries that wanted a certification that addressed the complete range of information security topics. The C)ISSO is based on many authoritative resources such as the ISO27001/2, the NIST guidelines (*www.csrc.nist.gov*), the Common Criteria ISO15408, and other leading references.

Mile2 describes the C)ISSO as: "Mile2's Certified Information Systems Security Officer - C)ISSO - program prepares and certifies individuals to analyze an organization's information security infrastructure in respects to threats and risks. This course helps you design a security program to mitigate risks relevant to today's business environment. Certified ISSO's are proficient in risk analysis, risk mitigation, application security, network security, operations security, business continuity, and disaster recovery planning."

The C)ISSO certification and examination have the following topic areas:

Module 1: Risk Management

Module 2: Security Management

Module 3: Authentication

Module 4: Access Control

Module 5: Security Models

Module 6: Operations Security

Module 7: Symmetric Cryptography and Hashing

Module 8: Asymmetric Cryptography and PKI

Module 9: Network Connections

Module 10: Network Protocols and Devices

Module 11: Telephony, VPNs, and Wireless

Module 12: Security Architecture

Module 13: Software Development Security

Module 14: Database Security

Module 15: Malware and Software Attacks

Module 16: Business Continuity

Module 17: Disaster Recovery

Module 18: Incident Management, Law and Ethics

Module 19: Physical

The C)ISSO examination is held online through computer-based testing. The examination, which consists of 100 multiple-choice questions, is expected to be completed by the candidate within two hours. A grade of 70% is required to pass the examination, and the candidate is advised of their score after the examination.

Training

Mile2 and their authorized affiliate-training partners offer an excellent range of training options, including live classroombased instructor-led courses, distance learning with a live instructor, videos, and student study materials.

Military personnel, retired veterans, and students are offered substantial discounts on training and examination costs.

The C)ISSO candidate should download a copy of the C)ISSO course and examination description from the Mile2 website at *http://www.mile2.com/mile2-courses/general-security.html*.

Certified Information Security Manager (CISM®)

The CISM examination and certification are offered by ISACA (*www.isaca.org*). ISACA describes the CISM as: "The management-focused CISM is the globally accepted standard for individuals who design, build and manage enterprise information security programs. CISM is the leading credential for information security managers."

The CISM examination is held twice per year (in June and December) at many locations around the world. The examination, which consists of 200 multiple-choice questions, is expected to be completed by the candidate within four hours. The examination is paper-based and held in conjunction with other ISACA examinations at the same time and in the same testing center as other ISACA certifications (CISA, CRISC, CGEIT). It is best to register early for the examination because the price of the exam rises as the exam date approaches, and the registration period ends several months before the examination date. Examination candidates register for the examination directly on the ISACA website, where the exam is offered in several languages.

The CISM is based on four main topic areas:

- Information Security Governance - 24% of the exam questions
- Information Risk Management and Compliance - 33% of the exam questions
- Information Security Program Development and Management - 25% of the exam questions
- Information Security Incident Management - 18% of the exam questions.

The examination is marked on a scaled score with a minimum mark of 200 to a maximum mark of 800. A score of 450 or better is required to pass the examination. Examination marks are sent to the candidates approximately eight weeks following the examination date.

A CISM must be endorsed by another professional that can attest to their years of experience in the field. A CISM must be able to submit proof of five years of work experience in the field of information security, with at least three years in the role of an information security manager.

A CISM is required to pay an annual fee for certification to ISACA and often a fee set by a local ISACA chapter. All CISM will be assigned to a local chapter if one is available.

The CISM must also attain and demonstrate at least 120 hours of Continuing Professional Education (CPE) credit during the three-year cycle of their certification with a minimum of 20 CPE hours in any one year.

The CISM must also agree to comply with ISACA's Code of Professional Ethics.

Training

CISM training is available through local ISACA chapters and other training providers. ISACA offers study books, sample questions, and online courses through the ISACA website.

A person interested in CISM certification can download a free CISM Bulletin of Information (BOI) from the ISACA website.

Certified Information Systems Security Professional (CISSP®)

The CISSP is administered by (ISC)^2®. The (ISC)^2 website is found at *www.isc2.org*. It is the authoritative source for all information regarding the CISSP certification, examination, and ongoing certification maintenance requirements.

(ISC)^2 describes a CISSP as: "A CISSP is an information assurance professional who defines the architecture, design, management and/or controls that assure the security of business environments. The vast breadth of knowledge and the experience it takes to pass the exam is what sets the CISSP apart. The credential demonstrates a globally recognized standard of competence provided by the (ISC)²® CBK."

The CISSP examination is hosted through computer-based testing at select Pearson VUE locations worldwide. The examination candidate can register for an examination through the (ISC)^2 website. The examination, which consists of 250 multiple-choice questions, is expected to be completed by the candidate within six hours. The examination candidate must select the ONE best answer from the four options provided. The examination is marked with a score from zero to 1000, and the candidate must attain a mark of 700 marks to pass the examination. In most cases, the candidate will be provided with their score after the examination.

The CISSP must have five years of experience (with some waivers for education degrees). However, a candidate that passes the examination but has less than the required experience level may become an Associate of (ISC)^2 and will have three years to complete the experience requirements. More so, another certified professional is required to endorse the CISSP candidate and authenticate his or her experience.
Once certified, the CISSP must attain and submit 120 hours of Continuing Professional Education (CPE) credits within the three years of their certification cycle. They must submit proof of at least 20 hours of CPE credit hours each year.

The CISSP must also pay the annual maintenance fee required by (ISC)^2. The CISSP may join a local (ISC)^2 chapter, but any local chapter fees are the responsibility of the local chapter and are not collected by (ISC)^2.

The CISSP must also agree to abide by the ((ISC)^2 Code of Ethics.

The eight domains of the CISSP are:

1. Security and Risk Management.
2. Asset Security.

3. Security Architecture and Engineering.
4. Communications and Network Security.
5. Identity and Access Management.
6. Security Assessment and Testing.
7. Security Operations.
8. Software Development Security.

Training

(ISC)^2 provides top-quality training for the CISSP through instructor-led sessions and live online distance learning. (ISC)^2 also provides support materials such as sample tests (studISCope), and textbooks through the (ISC)^2 website. Several other non-affiliated organizations also provide training for (ISC)^2 the CISSP.

A candidate interested in the CISSP should request a copy of the Candidate Information Bulletin (CIB) from the (ISC)^2 website. The CIB outlines the examination process and other information required for a CISSP candidate.

Studying for Certification

Regardless of the certification desired, the process of certification is challenging and requires extensive review and preparation. The examinations are designed to test both the knowledge and skill of the information security professional. This requires a level of comprehension that goes deeper than simply understanding and demands that the professional be able to demonstrate their ability to apply their experience and judgment in applying their knowledge in practical-based situations. Very few professionals have a level of experience that covers the entire range of information security topics addressed in the various certification examinations.

The first step in preparation is to review the information provided by the various certification bodies. The (ISC)^2 Candidate Information Bulletin, ISACA's Bulletin of Information, and Mile2's C)ISSO Course Outline. Every topic listed on these documents is likely to appear on the examination. By reviewing these outlines, the candidate can identify weak areas and thereby ensure that they have a chance to review and research those topics as a part of their study plan.

The next step in preparation is to set the exam date. In some cases, exams may sell out, and by registering for a set examination date, this can ensure that the study plan has a focus date, and the candidate knows that they will be able to sit for the examination at the time they are best prepared.

For many people, the best way to prepare is to attend an official training session. These courses provide an excellent overview of all topic areas and may fill in some of the gaps in the candidate's knowledge. Attending with a group of other students can also provide enhanced understanding and value through class discussion, debate, and additional study techniques. The secret to gaining the most advantage from training is to seek a way to focus solely on the training during the course period. When a student is juggling their regular work with the class, then they often lose focus and are unable to gain the most benefit from the course. The other secret is to prepare before the class. The student can review books or pre-class study materials - this allows them to become familiar with the terminology, concepts, and key areas so that the class becomes a review and reinforcement for their knowledge rather than an introduction to previously unknown topics.

Most candidates will benefit from an organized study plan that focusses on each topic area in a scheduled manner. Even more, selecting one topic area at a time allows the mind to focus on that area without jumping continuously from topic to topic in a disorganized manner. It must be remembered that activity is not a substitute for progress, and just flipping back and forth in pages in a book is not a substitute for really studying a topic and working with it until it is fully understood. The candidate should pay close attention to areas that are vague or poorly understood and seek to work on those areas until they are well-known and properly understood. You know a topic has become clear for you when you can describe it simply to another person. It is advised that you do not skip over the tough areas and just focus on the familiar - that is much easier from a confidence point of view but will leave significant holes in the study program and may lead to failure on the examination.

Remember that the examination is not based on simple knowledge. The candidate must be able to analyze the topic and options addressed in the exam question and, from that analysis, select the BEST answer. A thorough understanding of the topics and how to use (apply) those topics in a real-world setting is the key to success. When studying, it is important to link topics together - understand the relationships between topics, tools, procedures, and the linkage between information security and business objectives. Remember, the reason for the security is to support business requirements, not just to be secure.

Sample questions are often a good way to validate understanding. A question forces the candidate to consider all the angles, ensure a clear understanding of differences between various topics and answers, and verify that they have understood the core concept behind the question. Questions should be used for more than just reviewing one topic. Do the analysis to discover the BEST answer but also take the time to understand why the other answers are wrong or not as good. Review the "wrong" answers and explain what they apply to - many of the "wrong" answers are actually "right" for another question - think about what question each answer would be suitable for. Many of the sample questions that are out there are poorly written or are inaccurate - in many cases, the answers may actually be wrong, or the question is not of sufficient quality to be used in a real examination. Therefore, when a candidate disagrees with an answer - the candidate may be correct. So, use the questions to review and study, but do not necessarily use them as a tool to learn new topics. Sample questions do not go through the same review process as real examination questions, and sample questions will not appear on the real exams anyway - so to only get a sample question correct will not necessarily indicate examination success.

The test day

Do not arrive at the test center late, overtired, or over-stressed. The examination is based on analysis and the evaluation of each question, so to stay up late to cram in a few hours of extra study may be the worst choice to make. The exams are tough, physically, and mentally - it is hard to remain focused for the entire time, and to start exhausted is almost always a recipe for mistakes and lack of confidence.

Most tests require absolute punctuality and to arrive even a few moments late may result in denial of entry to the exam as well as the loss of examination fees. Plan to be at the test center a little early so that you can prepare, relax, maybe do a few moments of last-minute review and get comfortable before the start of the examination. Some paper-based examinations require you to bring a pencil and eraser to the examination. Be sure to bring a few pencils (usually, a paper-based examination will require a certain type of pencil) - a good quality eraser and perhaps even a snack or drink. Most examination rooms will not allow anything at the desk except for examination materials. Still, most will allow the candidate to take short breaks and go to the back of the room or just outside for a quick moment to grab a snack, drink, and a bathroom break. It is good to take frequent breaks during the exam - even if for only a moment or two to relax and refresh.

Set a study plan that works up to the examination date, do reviews as frequently as possible - even if to do only a few sample questions for ten minutes at a time, so that you can build on your knowledge.

Good luck, and congratulations on taking this step forward in your career. Even if a candidate does not pass the examination, there is little doubt that they have learned a lot and will have benefitted from the experience of preparation and review.

APPENDIX B:

CISSP Study Guide

Test Tips

- *This is a management exam. Questions are far more likely to ask you to choose the best solution than to provide a definition.*

- *Focus on this main concept: "What is the problem you are trying to solve?" Then ask, "Which alternative best solves it?"*

- *You will need to understand the technologies to answer those questions.*

- *Remember the golden rules listed below. These five fundamental truths will help you understand* *the security and will also help you pick the right answer on the exams.*

1. *The policy is the key to nearly everything*
2. *Training is mandatory*
3. *People safety comes first*
4. *Everyone is responsible for the security*
5. *Management buy-in is essential*

Information Security Risk Management

Principles and Requirements

- Requirements: functionality (what are the features?) & assurance (how well does it perform those features?)
- Security blueprint: best practices that form a comprehensive security policy program. A security architect figures out what the security needs of an organization are and creates a blueprint for the staff to follow.

Policy - Terms

- Standards: hardware & software to be deployed universally across organizations. Standards start with the phrase "We use…" as in "We use Dell laptops" or "We use Norton Antivirus."
- Procedures: step by step required actions.
- Baseline: minimum security implementations for specific platforms or environments. Baselines measure minimums as in "All our PCs have 1 GB RAM" or normal as in "Our e-mail server sends 1,000 e-mails per hour."
- Guidelines: recommended actions, best practices or suggestions
    - ISO 17799/27002
        - Based on British Standard (BS) 7799-1

        - Best practices/management checklist
    - BS 7799-2 / ISO 27001
        - Compliance document
        - Attainable certification

Organizational Roles and Responsibilities

- Executive Management: ultimately responsible for security.
- Information Systems Security Professionals: Design, implementation, management, review of policies, standards, procedures, and guidelines.
- Data / Information Owners: identify assets and assign labels.
    - Process owner = programmer, designer. They do not own the data, but they do own the engine it is running on.
- Custodians: maintenance responsibilities (e.g., network administrators/operations)
- Users.
- IS/IT functions: set up networks, desktops.
- IS Auditor: responsible for testing the effectiveness of security. In testing, they should go through the same process to gain access as a normal user. Auditors make sure your policies and procedures are followed. They also note shortcomings in

them concerning best practices or regulations.

- Good practices
    - If people go from a lower-level position to a higher level, make sure you tell them upfront if you are going to do a background check.
    - Least privilege: only give the permissions needed to do your job.
    - Need to know: only give the knowledge needed to do your job.
    - Separation of duties: defeats fraud. This forces collusion (when people in different departments have to conspire to pull fraud off)
    - Job rotation & mandatory vacations: helps detect fraud and defeats collusion. If you have to choose between job rotation and mandatory vacations to defeat collusion, job rotation is a better option.
    - Use top-down (i.e., starting with management) instead of bottom-up (i.e., consensus-based) planning. Bottom-up has no funding & no authority.
    - Provide training and education
        - Training: awareness/job skills.
        - Education: decision-making/security management skills.

Risk Management and Analysis

- Terms
    - Threat: potential danger.
    - Threat agent: source has the potential of causing a threat.
    - Exposure: damage factor. An instance of being exposed to losses from a threat. This is measurable.
    - Vulnerability: could be lack of countermeasure or weakness in countermeasure.
    - Risk: the likelihood of an unwanted event and the impact.
    - Residual risk: the portion of risk that remains after the implementation of safeguards/countermeasures.
    - Total risk: comprised of threats, vulnerabilities, and current asset value.
- Risk analysis – identify potential loss. This involves determining the value of assets and what can harm them. Risk analysis should be top-down and repeatable.
    - Single loss expectancy (SLE) = Asset Value $ x Exposure Factor %
    - Probability: the annual rate of occurrence (ARO).
    - Annual loss expectancy (ALE) = SLE x ARO

- Risk management: to reduce or mitigate the potential loss. This involves the following:
    - Risk analysis
    - Cost/benefit analysis
    - Deploying safeguards
    - Auditing
    - Insurance
    - Continuity planning
    - Training, etc.
- Use legal, HR, and auditors to consult regarding regulatory & compliance issues
- Quantitative risk analysis = numeric
- Qualitative risk analysis = subjective, scenario-orientated. The disadvantage to qualitative is that it is not as accurate, management might not agree, and it is difficult to assign dollar amounts.
- Other risk analysis methods
    - Failure modes and effects analysis (FMEA): potential failures for each mode.
    - Fault tree analysis – a.k.a. Spanning tree analysis. Create a tree of all threats.
    - Delphi – an anonymous survey.
- ANZ 4360 standard – standard for qualitative risk management from new Zealand
- Remedial selection measures.
    - Risk reduction: provide countermeasures.

        - Risk transference: a.k.a. Risk-sharing (insurance)
        - Risk acceptance: accept risk (document & acknowledge)
        - Risk avoidance: avoid the environment to avoid the threat (e.g., banning all wireless networks)
    - You should not put all countermeasures in one box as this is a single point of failure, and it is rare for one solution to be good for everything.

Ethics

- Teleology: ethics of purpose or goal. The greatest good to the greatest number
- Deontology: ethics of duty. For example, religious.
- Code of Ethics
    - (ISC)^2
        - Protect society, commonwealth, and infrastructure (People).
        - Act honorably, honestly, justly, responsibly, and legally (Law).
        - Provide diligent and competent service to principals (Organization).
        - Advance and protect the profession (CISSP).
    - RFC 1087: access and use of the Internet is a privilege.
        - Internet Activities Board (IAB): defines what is unacceptable/unethical. Unethical:

- Seek to gain unauthorized access
- Disrupt the Internet
- Waste resources
- Destroy integrity
- Compromise privacy
- Involves negligence

Security Architecture and Design

Enterprise Security Architecture

- Goals can be strategic (long term), tactical (midterm), or operational (short term)
    - Note that the labels (strategic, tactical, and operational) can vary from different sources. The important point is that at the lowest level are the people who do the job, at the mid-level are the people who manage the job, and at the top level are the people who decide what job to do. CISSPs are typically at the mid or top levels.
- Your solutions approach can be enterprise solutions (with management support) or point solutions (no management support).
- Deming was the "father" of total quality management (TQM)
- Zachman framework: two-dimensional classification scheme (levels of architecture & levels of interest).
- Other frameworks include COBIT, COSO, ITIL, CMMI, SEI IDEAL, TOGAF, and ISO 42010:2007.

Common Computer Architecture

- CPU States

    - Supervisor state: the program can access the entire system
    - Problem/user/program state: only non-privileged instructions executed (applications).
    - Process states: stopped/operating, wait/running, masked/interrupt.
    - If a vulnerability is exploited to any module/process thread, it will affect all applications that use it.
- Operating System support for applications
    - Multitasking: Concurrent or interleaved execution of multiple tasks.
    - Multiprogramming: rarely used the term. Interleaved execution of multiple programs.
    - Multiprocessing: parallel processing.
    - Multiprocessor: more than one processor.
    - Multicore: more than one processor on a single chip.
- Memory Management
    - Primary storage: CPU, memory, input/output.
    - Secondary storage: Storage devices.
    - If using virtual memory, you need both storage and memory.
    - Memory addresses can be logical, relative, and physical.

    - Page fault: The signal saying the page is not in primary storage but is in secondary storage. This is not a problem.
    - Page fault error: The system cannot find the page in RAM *or* on HD.
- Trusted Computing Base (TCB)
    - The totality of protection mechanisms that are responsible for enforcing a security policy.
    - Subjects: active entities like users or programs accessing data.
    - Objects: passive entities like files/data.
    - Reference monitor: An abstract machine that examines all requests from a subject for access to an object and determines if that request is allowed. The determination of the access is made by consulting the security kernel, which may consist of such things as access control lists, LDAP database, password file, authentication server, etc.
    - Security kernel: hardware/software elements of TCB that implement reference monitors.

Computer Architecture Protection Concepts

- Process isolation preserves an object's integrity and the subject's adherence to access controls. It prevents objects from interacting with each other.

  - Example: time multiplexing, naming distinctions (SSID), virtual mapping (memory space)
  - This can be accomplished through layering. Processes in one layer cannot communicate with another layer (except through a secure interface)
  - Data hiding: when there is no interface to communicate between layers. This protects both confidentiality and integrity.

- Ring protection
  - Ring 0 – O/S Kernel
  - Ring 1 – O/S
  - Ring 2 – Utilities
  - Ring 3 – User applications
- Security domains (a.k.a. Execution domains, protection domains): a group of subjects (processes) that share similar privileges or management controls.

Operating System Protection Concepts

- Discretionary access control (DAC): object access is left to the owner.
- Mandatory access control
  - Need an access control policy.
  - Need labeling (classification) for objects.

    - Need clearance/privilege labels for subjects (assigned by management but implemented by system administrators).
- Trusted path: a secure login or authentication process that is not easily compromised.
- Clipping: Setting the audit level by deciding what to log or not log.
- Filtering: looking at a subset of the existing logs
- Object reuse protection: protecting against memory leakage and data remanence. (residual data on magnetic media)

Evaluation criteria

- Certification: the solution meets the requirements. Certification is the sign off by IT staff that a solution meets the current requirements.
- Accreditation: management approval. It includes management's permission to implement and acceptance of risk.
- Trusted Computer System Evaluation Criteria (TCSEC)
    - Orange book (part of rainbow series)
    - TCSEC only tests confidentiality
- Trusted Network Interpretation (TNI) – the red book of the rainbow series. Applies orange book principles to network systems.

- ITSEC – European standard
  - Functionality & Assurance
  - Tests all three of A.I.C. triad
- Common Criteria (international) IOS 15408
  - A Common Criteria (CC) lab will test a product against a MANUFACTURER's specifications. If one firewall vendor says they can do 1,000 transactions per second and they only do 1,001, they will get a good evaluation on that point. However, if another vendor says they can do 5,000, and they only do 4,500, they will fail.
  - Establishes a framework for each industry through protection profiles (PP).
  - Covers all three of A.I.C. triad.
  - Uses evaluation assurance level (EAL).
  - Security target: the protection profile (PP) that will be selected for testing a product.
  - The target of Evaluation (TOE): entity under testing.

Security Models

- Bell-Lapadula: confidentiality model (*read down and write up*).
    - “state” machine model.
    - Simple security property: subject cannot read an object of higher sensitivity.
    - Star property (*): subject cannot write lower
    - Strong Star: cannot read/write to the object of higher/lower .
    - Does NOT address the "need to know" of the user.
- Biba Integrity: integrity model (*read up and write down*)
    - Simple integrity: cannot read down.
    - Integrity star * property: cannot write higher.
    - Invocation property: cannot invoke execution up.
    - 1st Goal of Integrity - Unauthorized users make no changes.
    - Access tuple: Subject and Object
- Clark & Wilson: integrity model
    - Reaffirmed Biba's first goal of integrity.
    - Postulated the second goal of integrity - "Authorized users make no unauthorized changes."

    - Offered the concept of "Separation of Duties" as an assurance mechanism for this functional requirement.
    - Internal and External Consistency.
        - Internal consistency: the transaction must fit the internal parameters of the system.
        - External consistency: the transactions must fit the real world.
    - Access triple: subject – program – object
- Access control matrix.
- Lattice: Information flow matrix.
- Brewer and Nash Model / Chinese Wall.
    - More of a policy model.
    - Chinese wall – the doctor should not tell patient A about patient B.
- Graham-Denning Model – uses 'monitor' (rule checker).
    - James Anderson calls this a 'reference monitor.'
- Harrison-Ruzzo-Ullmann – uses an access matrix (another name for a reference monitor.)

CRYPTOGRAPHY

Terms

- Cryptogram: ciphertext.
- Cryptanalysis: defeating cryptology.
- Keyspace: number of distinct keys.
- Key clustering: Uneven distribution of key use across keyspace.
- Key collision: Two different users of the same key OR two different keys that will:
  - Generate the same ciphertext.
  - Decrypt a single ciphertext.
- Work factor: the amount of time to overcome a protective measure, measured in a million instructors per second (MIPS).
- Link encryption: Creates a new header, hides the source/destination address, and provides traffic flow confidentiality.
- End-to-end encryption: you lose traffic flow confidentiality. Used with Key Distribution Center (KDC).
- Scytale-Sparta: 400 B.C. method of encrypting using a rod.
- Caesar Cipher: rotational cipher of 3 characters
- Alberti's Disk: rotation using disks.
- Kerchkhoff principle: the strength of your encryption should not rely on keeping your

algorithm secret; it should instead rely on the secrecy of your keys.

- Feistel: developed Lucifer, which later became DES.
- Wassenaar agreement: export rules based on key length.
- Moore's law: processing speed doubles every 18 months.
- IV: initialization vector.
    - Some variations of block algorithms need the output of the previous block to process the current block. The IV represents the “previous” block while processing the first block.
    - For stream algorithms, the key is often constant. To make the keystream different for each use, and IV is employed to modify the key before feeding it to the keystream generator.

Encryption Systems

- Cryptographic algorithms
    - Symmetric
        - Block
        - Stream
    - Asymmetric
        - Discrete logarithms
        - Integer factorization
- Substitution cipher: Caesar (shift alphabet or scramble).

- Transposition (rearrange letters; use a table).
- Polyalphabetic cipher (use several different alphabets).
    - Vigenere cipher
- Running Key Cipher: uses a book.
- One-time pad: only algorithm provably unbreakable by exhaustive search because the key is only used once. A.k.a. Vernam cipher. E.g., time-stamped synchronous tokens.
- Concealment cipher: true letters concealed (e.g., words in a paragraph).
- Steganography: uses the least significant bit (LSB)

Methods of Encryption

- Stream cipher
    - RC4
    - Uses XOR exclusively
    - Usually implemented in hardware. Hardware is always faster than software.
    - The key goes into a keystream generator (KSG). The keystream generator takes a key (often a word or a phrase) and uses it to generate a never-ending, never-repeating series of balanced zeroes and ones.
    - The plaintext and ciphertext are of the same size

- Block cipher
  - Fixed-size blocks
  - Example: DES (64-bit), AES (256)
  - Block cipher (in all modes) is always slower than a stream cipher because it is typically implemented in software instead of hardware and because it has more work to do.
    - While block ciphers are slower than stream ciphers, all symmetric ciphers (stream and block) are always faster than asymmetric encryption.
  - 5 modes. Two are block modes where the encryption algorithm is used to convert the plaintext directly to ciphertext. The other three are stream modes where the algorithm is used solely as a keystream generator. The plaintext is then converted to ciphertext by mere XOR operations.
    - Block mode: Electronic Code Book (ECB)
      - Typically used for encrypting small independent blocks of information.
      - Easier to crack than others.
      - Fast.

        - Susceptible to plaintext attack.
        - Uses the same key for each 64-bit block.

    - Block mode: Cipher Block Chaining (CBC)
        - Used for encrypting documents, files, and storage media.

  - Stream Mode (block ciphers can have stream characteristics): Cipher Feedback (CFB)
        - Used for encrypting streaming communication (VPN, phone, vide).
        - Faster than CBC.

- Stream mode: Output feedback (OFB)
    - Used for encrypting streaming communications
    - Faster than CFB.

- Stream mode: Counter (CTR)
    - Used for streaming communication.

- Uses a large random number.
- Can do parallel pre-processing of keys.

Symmetric Systems

- Types
    - DES, 2DES, 3DES.
    - AES (Rijndael).
    - IDEA.
    - RC4 (stream), RC5, RC6.
- Uses private key (old name), single key, shared key, session key, secret key.
- Key is often delivered out-of-band (non-technical means and away from the primary system).
- Strengths: fast.
- Weakness: key management & distribution.
- Does not provide proof of origin or non-repudiation because both sides use the same key.
- DES
    - 64-bit input and output block size.
    - 56-bit key + 8 parity bits.
    - 16 rounds of transposition (a.k.a., permutation) & substitution.
- 2DES
    - 112 bits (two 56 bit keys).
    - Susceptible to a meet-in-the-middle attack.
- 3DES

  - 3 56 bit keys (168-bit key length)
  - DES-EEE3: 3 different keys
  - DES-EDE3: Encrypt, decrypt, encrypt (3 different keys)
  - DES-EEE2: Encrypt with Key1, Key2, then Key1 again.
  - DES-EDE2: Encrypt with Key1, decrypt with Key 2, encrypt with Key1 again.
- AES (Rijndael)
  - Advanced encryption standard that won the competition.
  - 3 different key sizes (128, 192, 256)
- RC4 – STREAM cipher (Rivest) – used for VPNs, wireless, SSL.
- RC2, RC5, RC6 – block ciphers (with choices of block size, key size, and rounds); e.g., RC5-64/12/32 (RC5 with 64-bit block, 12 rounds of substitution and transposition, and 32-byte key).
- Blowfish – key length up to 448 bits; block size 64 bits.
- Twofish – 256-bit key length.

Asymmetric Systems

- Public/Private keys.
- Uses a trap-door one-way function (i.e., the inverse is easy given a secret piece of information).
- Three formats:

    - Secure message format – encrypt with receiver's public.

    - Open message format – encrypt with sender's private (to authenticate sender).

    - Secure and signed message format – encrypt with the sender's private *than* with receiver's public (remember the order). Think soft center with a hard, crunchy shell.

- Strengths: confidentiality, access control, authentication, integrity, non-repudiation.
- Weaknesses: computationally intense, slow.
- Public Key / Asymmetric approaches:
    - Prime factoring
        - RSA: 512, 768, 1024 bit keys. Encrypts & provides digital signatures for non-repudiation.
    - Discrete logarithms.
        - Diffie-Hellman (DH): only used for key exchange.
        - Elliptic Curve Cryptosystems (ECC): algebraic points on an elliptic curve. Faster and has smaller key sizes.
        - Digital Signature Standard (DSS).

        - El Gamal – like RSA but unpatented.
        - LUC.
    - Others
        - Merkle-Hellman Knapsack (broken).
        - Chor-Rivest knapsack (broken).

Hybrid Systems – PGP, S/MIME, VPN/SSL. Hybrid systems use symmetric for bulk data encryption and asymmetric for key distribution.

Message Integrity Controls

- Accidental change detection is done through parity, hashing, and checksums.
- Intentional change detection is done through digital signature, HMAC, and CBC-MAC.
    - CBC-MAC
        - Hash the ciphertext
        - Encrypt the ciphertext using Cipher Block Chaining (CBC).
        - Take the last encrypted hash block and encrypt it again.
            - Note: WPA2 the message is considered a "frame," not a block
        - That value becomes the message authentication code

        (MAC) that is used for verification.

- Hashing
    - MD2, MD4, MD5 – 128 bits.
    - SHA-1 – 160 bits.
    - SHA 256, SHA 384, SHA 512.
    - Haval – 128, 160, 192, 224, 256 (5 key sizes).
    - RIPE MD-160, RIPE MD-128 (European).
    - Tiger.
    - The larger the fingerprint size, the more secure because there is less chance of collision.
    - The smaller size could leave it vulnerable to a birthday attack (50% chance 1 out of 23 shares same b-day). A birthday attack is when you look for two messages that produce the same hash (collision).

Digital Signatures

- Used to verify origin and sender.
- The private key signs and the public key verifies.

- The signature is created by encrypting a digest (hash value) of the message with the private key.
- Benefits: non-repudiation of origin & sender. It can also use with a signed receipt of the original hash for non-repudiation of receipt & delivery. It also provides integrity because of hashing.
- Types
    - RSA
    - El Gamal
    - Fiat-Shamir
    - Schnorr
    - Nyberg-Rueppel
    - Digital Signature Standard (DSS)
        - SHA-1
        - Digital Signature Algorithm (DSA)

Certification

- X.509 standard.
- Certificate authority: manages certificate lifecycle; a trusted third party.
- CRL: certificate revocation list.
- Internal certificates (i.e., in-house certificates) are typically issued by human resources or by that personnel responsible for issuing building badges.
- The certificate includes version, serial number, algorithm types, issuer, valid dates, name of the owner, public key,

issuing CA ID, subject ID, and digital signature.

Public Key Infrastructure (PKI)

- Provides the foundation for secure e-business.
- A method for distributing trusted keys.
- Provides confidentiality, access control, integrity, authentication, non-repudiation.
- Public keys published as certificates.

Key Management

- The key-encrypting keys must be separate from the data keys.
- Key escrow: the third party holds on to keys.
- Key distribution center (KDC):
    - End-to-end encryption
    - Each user gets a key

Cryptanalysis and Attacks

- Ciphertext only attack:
    - You have a sample of ciphertext only.
    - Hardest.
    - The object is to crack one message.
- Known plaintext attack:
    - You have ciphertext & corresponding plaintext.
    - Object is to get the key.
- Chosen plaintext attack:

    - The attacker can trick or induce opposition into encoding the plaintext of the attacker's choice. The attacker can capture the ciphertext and use it along with the plaintext to discover the key.
- Adaptive chosen-plaintext attack:
    - Similar to chosen-plaintext but the attacker has repeated the ability to encode plaintext of choice. This requires access to the cryptosystem with the key loaded.
- Chosen ciphertext attack:
    - Use against public-key cryptosystems.
    - You can choose a piece of ciphertext and can obtain the corresponding decrypted plaintext (free use of cryptosystem to decrypt but cannot get decryption key).
- Adaptive chosen ciphertext attack:
    - An adaptive version of chosen-ciphertext.
- Man-in-the-middle.
- Side-channel attacks:
    - Looking for something computationally intense.
- Brute force (takes time & money).
- Birthday attack (looking for collisions).
- Attacks on Symmetric Block Ciphers (e.g., DES):
    - Differential Cryptanalysis.

        - Chosen plaintext.
        - Examine probabilities of each key in comparison with two plaintexts that have been encrypted.
    - Linear Cryptanalysis:
        - Known plaintext.
        - Given enough pairs of plain/ciphertext, you can figure out the key.
    - Differential linear cryptanalysis (combination).
    - Algebraic attacks.
- Other attacks include purchase-key (bribery), rubber-hose, social engineering, and implementation (WEP, Netscape) attacks.

E-mail Security

- PEM, PGP, MOSS, S/MIME, MSP.

Internet Security

- 3D Secure
- Currency Cards
- SET
- SSL
- S-HTTP
- IPSec
- SSH

Steganography

- Physical steganography: e.g., invisible inks.
- Null ciphers: adding non-cipher characters (nulls) to hide plaintext.

Physical Security

Introduction

- Safety of people is always the primary concern.

Layered Defense Model

- Multiple obstacles.
- Disadvantages: how do you get out in a timely fashion**,** false sense of security, and complexity through high cost?

Crime Prevention through Environmental Design

- Remember S.A.T.:
  - S=Surveillance.
  - A=Access control.
  - T=Territoriality.
  - People will watch (S) and limit access (A) to areas or property (T) that they consider their own.
- Remove anything that would encourage crime.
- Put controls that would deter crime.

Site Location – be sure to analyze the site location to limit the likelihood of riots, crime, natural disasters, etc.

Doors

- Should be lit for cameras.
- Do not block exit doors.

Windows

- Tempered glass – mixed with other substances.
- Acrylic materials – mostly plastic; stop conventional bullets.
- Polycarbonate windows – combo of glass and acrylics.
- Laminated – layers of plastic.
- Wired – schools, hospitals, etc.; broken glass does not shatter.
- Solar window films.
- Glass breakage sensors.

Infrastructure Support Systems – make sure you have redundant electricity and air conditioning (HVAC).

Fire

- Fire will spread faster in cubicle environments.
- Make sure you do drills after hours and on weekends (drill should include headcount, emergency exits, and a safe passageway).
- Smoke detectors:
  - Ionization types – detect charged particles in smoke.
  - Optical / Photoelectric – react to light blockage caused by smoke.

    - Fixed/rate-of-rise temperature – heat detectors.
    - Suppression is concerned with interfering with fuel, heat, oxygen, or chemical reaction.
- Fire types and suppression
    - A (Ash):
        - Common combustibles, water, paper, clothes, etc.
        - Water, foam, dry chemicals.
    - B (boil):
        - Liquid, kerosene, gas.
        - Gas, CO_2, foam, dry chemicals.
    - C (computer):
        - Electrical.
        - Gas, CO_2, dry chemicals.
    - D (dilithium):
        - Metals, magnesium, lithium, uranium.
        - Dry powders.
    - K (kitchen):
        - Grease fires.
        - Wet chemicals.
- CO_2 Suppression: can kill you.
- Halon gas – the chemical reaction of fire produces chemicals that can harm you:
    - Montreal Protocol eliminates Halon.
    - Substitutes:
        - FM200:
            - Most effective.

            - Uses same sized tanks, piping, nozzles, etc. Uses the same quantities. Therefore, it is good for replacement.
            - Materials cost is highest among all other alternatives, so it is typically used for replacements and not new installations.
        - CEA 410
        - FE 13
        - NAF S-111
        - ARGON
        - ARGONITE
        - INERGEN
        - Water in the form of mist.
- Water sprinkler systems:
    - Wet pipe: pipes contain water under pressure; water automatically discharges from open sprinklers. Problems occur when the temperature goes below freezing or if there is an accidental discharge.
    - Dry pipe: pipes contain air under pressure; fire causes sprinklers to open and air pressure to drop and water valve to open.
    - Pre-action: pipes contain air under pressure; a supplemental detection

system opens the water valve to release water into the pipes (relies on the secondary system).

- Water threats – don't have pipes above server room; don't put datacenter in basement.
- Power threats:
    - Have emergency power off (EPO).
    - Blackout – prolonged loss of commercial power.
    - Fault – a momentary loss of power.
    - Brownout – reduction of voltage by the utility company for a prolonged period.
    - Sag/Dip – short period of low voltage.
    - Surge – sudden rise (not as sharp as a spike).
    - Transients – line noise that causes fluctuation in power.
    - Inrush current – an initial surge of current when there is an increase in power demand.
    - Electrostatic discharge – static electricity.
    - Noise – EMI & Radio Frequency Interference (RFI).
    - Countermeasures – backup generators and UPS (most have both because generator takes a while to activate).
- Heating/Cooling:

    - Recommended humidity: 50% +/- 10%.
    - Humidity too high: condensation.
    - Humidity too low: static electricity.
    - The temperature should be 70-75F. Remember, the temperature inside the computer is about 30 degrees higher than outside the computer.
- Perimeter security:
    - Includes fences, layered, natural, landscaping, gates, bollards, sensors, CCTV.
    - Sensors types
        - Photoelectric
        - Ultrasonic – sounds
        - Microwave
        - Passive infrared (PIR)
        - Pressure-sensitive
        - Capacitance – senses changes in the electrical field of a tightly monitored area.
        - Acoustical/seismic sensors – sounds or vibrations.
    - CCTV:
        - Not recommended for wireless LANs
        - Considerations:
            - PTZ: pan, tilt, and zoom
            - Transmission media consideration: coax cable can cause

        problems with fluorescent lighting.
        - CCTV is no good unless you are monitoring it.
        - Don't use a motion detector in the high traffic area.
        - Focal length: field of view. A lower number has a wider field of view.
        - F-Stop number: lens aperture (i.e., the depth of field). A lower number means a wider opening, and more light enters. A higher number means smaller aperture, a stronger area of focus, and less light entering. Therefore, if it is a smaller aperture, you will need to make sure it is well lit.
    - To monitor multiple locations, use pan and tilt units, panning devices, switches, and multiplexers (multiple cameras on single videotape).
- Lighting:

        - Continuous lighting considerations: glare protection (deliberately blinding), floodlighting.
        - Trip lighting (motion).
        - Standby/emergency (such as when the power goes out).
- Guard stations:
    - Preventive: presence.
    - Detective: check ids, monitor cameras.
    - Corrective: respond to alarms.
- Datacenter:
    - Make sure walls are not part of external building.
    - Walls should extend floor to ceiling (no raised floors, ceilings).
    - Include drainage for sprinklers.
    - For backup tapes, don't put in fire-proof safe because they are typically graded for paper, not backup media.
    - Make sure to include training as to how to handle tapes.

Access Control Systems and Methodology

Terms

- IAAA:
    - Identification: the assertion of identity.

    - Authentication: proof of the assertion.
    - Authorization: what a user can do.
    - Accounting: logging.
- Data remanence = data remains even if deleted (i.e., what is left on the drive after deleted).
- Security domain = group of subjects that share similar privileges or management controls.
- Capability tables = authorization table.

Control Categories

Tip: Identify which controls are done before the fact (e.g., deterrent) and which are done afterward (e.g., corrective). When reading a question, determine if it is asking about a before or after the fact control and then choose the answer accordingly.

- Deterrent: discourage incident
    - Administrative: policy.
    - Technical: warning banner.
    - Physical: beware of dog sign.
- Preventative: avoid an incident
    - Administrative: user registration procedure.
    - Technical: password-based login, IPS.
    - Physical: fence.
- Detective: identify incident
    - Administrative: review violation reports.
    - Technical: logs, ids.

    - Physical: CCTV.
- Corrective: remedy & restore controls
    - Administrative: termination.
    - Technical: unplug, isolate, and terminate the connection.
    - Physical: fire extinguisher.
- Compensating: alternative controls
    - Administrative: supervision, job rotation.
    - Technical: logging, keystroke monitoring.
    - Physical: layered defense.
    - Note: compensating is an <u>alternative when a primary is unavailable</u>. For example, to have a procedure to check ID when a badge reader is malfunctioning. All of the compensating controls also belong in other categories.
- Recovery: restore to normal
    - Administrative: DR plan.
    - Technical: tape backups.
    - Physical: reconstruction, rebuild.

Types of Authentication

- Asynchronous token device:
    - Time is not an issue with asynchronous token devices. These steps can take moments or minutes/hours/days, etc.

1. Request sent to authentication server along with user ID.

    2. Challenge sent from server to client.
    3. A client enters the challenge on the token device.
    4. Client reads response.
    5. Client enters response.
    6. Response sent to the server.
    7. The server verifies response with the user profile database.
  - Synchronous:
      - Careful timing is essential; else the login will fail
    1. A user sends a one-time password (pin on synchronous device + time = one time password).
    2. Authentication server housing the user profile database knows the symmetric key of the device. The server opens a one-time password, and if the time is the same, there is a match, and the user is authenticated.
  - Smart cards:
    - Memory chips – storage devices that cannot process information
    - Microprocessor chips – like having a miniature computer on a card
- Biometric:
    - Much more efficient for authentication (verification) than identification (assertion).
    - Physiological (e.g., fingerprint) or behavioral (e.g., keystroke).
    - Accuracy:

        - Type I Error: False Rejection Rate (rejecting people who should be accepted).
        - Type II Error: False Acceptance Rate (accepting people who should be rejected).
            - Mnemonic tip: Type <u>II</u> = accept
        - Cross-over error rate (lower number is more accurate).
- Kerberos:
    - No password is sent; instead, the password is only used as a key (therefore no eavesdropping on the password).
    - Authentication starts at the client's workstation.
    - Operation:
        - George logs on with user-id.
        - George requests a *Ticket Granting Ticket (TGT)* and sends the *session key* using user-id
        - A Kerberos *authentication server* (AS), which is part of the *key distribution center* (KDC), grants ticket-granting ticket (TGT) and sends the session key. It encrypts the message using George's password as the key.
        - George enters his password to get the ticket-granting ticket (TGT) and session key.

        - AS sends a ticket-granting server (TGS), also part of the key distribution center (KDC), service ticket using TGT. This is encrypted with the session key.
        - TGS grants service ticket #1, encrypts with the session key, and sends it to George.
        - George requests service with ticket #1 using a service ticket to application server #1.
        - For access to another application server, repeat the last three steps.
- SESAME:
    - Europeans developed this as an improvement to Kerberos
    - Uses public-key cryptography
    - Uses privileged attribute certificate (PAC) instead of Kerberos tickets

Access Controls

- ▪ Discretionary Access Control (DAC):
    - Classification labeling of objects by owner.
- ▪ Mandatory access control (MAC):
    - Uses sensitivity labels.
- ▪ Rule-based access control:
    - Example: firewall or router access lists.
- ▪ Role-based access control (RBAC):
    - Based on job functions.

- Content dependent access control:
    - Access based on what you need to do to a record.
    - Often applied to DBMS (Databases).
- Constrained user interface:
    - Restricts users' access to functions.
    - Often used by evaluation software, pay per view TV, public systems.
- Temporal / time-based isolation:
    - Each level takes a time slot (good for different requirements during backups).
- Centralized access control – RADIUS, TACACS+, DIAMETER.
- Decentralized access control (peer to peer, workgroups).

IPS & IDS

- Network-based or host-based.
- Signature-based / knowledge-based / pattern matching / stateful machine engine OR anomaly-based / behavior-based engine (protocol, traffic, or statistical anomaly).

Penetration Testing

- Zero-knowledge (black box); partial knowledge (gray box); full knowledge (white box).
- External vs. Internal; blind, double-blind (both sides don't know) vs. Targeted (both sides know, focused objective).

Application Security

Terms

- Transaction persistence = maintain transaction across all systems (gives you the ability to roll back).
- Hierarchical DBMS = parent/child relationship, easy to search.
- Network DBMS = hierarchical with a network of links. Includes records and sets (sets define the relationship between record types).
- Relational DBMS = tables & relationships).
    - Atomic = every row/column is exactly one data value.
    - Columns = attributes or fields.
    - Rows = tuples or records.
    - Data Definition Language (DDL) = used to create and delete database views and relations.
    - Manipulation language = used to construct database queries and modify data.
    - Entity integrity = Two rules. 1) primary key cannot be empty; 2) primary key must be unique.
    - Referential integrity = every entry in the foreign key must correspond to an entry in the primary key of another table.
    - Deadlocking / deadly embrace = when two or more processes are waiting for the other to do something to release a lock.

- OODBMS = object-oriented DBMS (no longer restricted to tables; can be audio, video files, etc.).
- ORDBMS = hybrid of OODBMS and RDBMS (tables can support binary data like video).
- Inference = putting together pieces of accessible data to arrive at supposedly secret information.
- Aggregation = intelligence gathering by combining data from lower classifications to derive information of a higher classification. The sensitivity of the whole is greater than the sensitivity of individual parts.
- Data warehouse = consolidated view of enterprise data, optimized for reporting and analysis. It is often used with data mining.
- Datamart = more focused than a data warehouse; is a specialized data repository for a specific department.
- Normalize the data = getting rid of duplicates.
- Metadata = information about data.
- Lock controls = control read/write access and ensure 1 user at a time
    - ACID = atomicity, consistency, isolation, durability
        - Atomicity = all changes take effect, or none do.
        - Consistency = transaction only allowed if it meets integrity constraints.

        - Isolation = results are not visible until transaction is complete.
        - Durability = completed transaction is permanent.
    - Mnemonic:
        - All: all or none.
        - Changes: consistency maintained during change
          [are]
        - Invisible: in-progress changes are hidden
          [until]
        - Done: when you say it's done, it stays done even in the event of a crash.
- OLTP = online transaction processing:
    - Security concerns are concurrency and atomicity
        - Concurrency = two users cannot simultaneously change the same data
        - Atomicity (defined above as well) = if one step fails, all steps should not complete.
        - Often uses journaling (back up in real-time) and transaction logs to do this.
    - OLTP systems use 2 phase commit process:
        - 1) write across all databases.
        - 2) commit to all databases.
        - Ensures atomicity.

- View-based access controls = security through views.
- Knowledge discovery in databases (KDD) = method of identifying valid and useful patterns in data. Some use Artificial Intelligence (AI).
    - Types
        - Probabilistic approach.
        - Statistical approach.
        - Classification approach.
        - Deviation and trend analysis.
        - Neural networks.
        - Expert system approach = algorithms that infer new facts from knowledge.
        - Hybrid approach.
    - External consistency = You should verify decisions based on expected outcomes.
- Object reuse = an object may contain sensitive residual data.
- Garbage collection = de-allocation of storage following and during program execution. Garbage collection is to RAM as defragging is to a hard drive.
- Trap doors/back doors = hidden mechanisms that bypass authentication measures.
- Time of Check / Time of Use (TOC/TOU) = Security risk that exploits the discrepancy of when a security function checks the contents and when the variables are actually used. For example, if a logged-in user's account is

deleted, that user may still retain access as of login-time rather than the current time.

- Executable content / mobile code = web applets (javascript), dynamic e-mail.
- Virus = malicious code that replicates by attaching itself to other programs or files.
- Worms = malicious and continuous process that reproduces and hogs up resources. This often does not involve the user.
- Multipartite virus = hybrid of different virus types
- Trojan horse = malicious code that pretends to be something fun or useful.
- Logic bomb = malicious code that is often planted by insiders and waits for a condition or time.
- Data diddlers = malicious code that corrupts programs or data a tiny bit at a time, so it doesn't go detected. Backups will not protect you against this.
- Maintenance hook = back door, a hidden mechanism that bypasses controls.
- RAT = remote administration tool (good), remote access Trojan (bad).
- Rootkits = a series of Trojan horse programs that can replace critical system files or interfere with kernel functions.
- Easter eggs = a hidden surprise function in a program

- Spyware = a program that sends information about your web surfing habits to a particular web site.
- Adware = a program that periodically pops up ads on a user's computer based on the user's surfing habits.
- Botnets = used for DDoS or SPAM.
- Phishing = a scam to steal personal information typically using e-mail as the bait.
- Regression testing = retesting after changes (best to test all components).
- Certification = testing the features and safeguards of a system to decide if it is suitable for deployment in the organization. Sign off by IT staff that a program meets the needs of an organization.
- Accreditation = management's acceptance of a safeguard and risk.

System Life Cycle

- Security should be in the beginning and be included in each stage.
- Typical phases:
  - Start-up/initiation and planning.
  - Acquisition & development/analysis and design
    - Programming and testing.
    - User acceptance testing.
    - Certification and accreditation.
  - Implementation = roll out to production.

  - Operations and maintenance = change control & updates, enhancements.
  - Decommissioning = transitioning to something better.
- SLC is different than SDLC (system development life cycle) in that SDLC does not include anything past turnover to production.

Programming Languages

- 1GL – machine language (machine-oriented binary code that is hardware-specific).
- 2GL – assembly language (human-readable, hardware-specific).
- 3GL – high-level language (machine-independent, C, C++).
- 4GL – very high-level language (application-specific, SQL, macros).
- 5GL – natural language (typing/speaking and have the system perform).
- Assembler = translates assembly to machine.
- Compiler = translates high-level into machine language (note: *machine* language, not assembly).
- Interpreter = translates instruction-by-instruction for testing. Interpreted languages are platform-independent.

Object-Oriented Programming

- Classes = how to make objects (like recipes).
- Objects = instance of the class.

- Message = objects send to other objects.
- Instantiation = act of creating objects using classes.
- Inheritance = inheriting data and functionality from other objects.
- Polymorphism = different objects respond to the same command in different ways.
- Polyinstantiation – two definitions.
    - Programming = creating a new version of an object by replacing variables with other values.
    - Security/countermeasures = creating different versions of the same information for different classification levels. The goal is to prevent users at a lower level from discovering what is really going on at a higher level.
- Common Object Request Broker Architecture (CORBA):
    - Provides a messaging environment for objects from different platforms and different languages to locate and exchange information with each other.
    - Client objects create client stubs, which interact with object request broker; server objects create server skeletons, which interact with object request broker.

Software Protection Mechanisms

- Isolate production and programming environments
- Keep purchased software in escrow (in case they go out of business).
- Heuristic scanning – watching for small but suspicious code strings.
- Change detection software = tripwire.
- Edit controls = entering in invalid data.
- Do not use production data in testing systems.
- Sanitize test data (clean out confidential information). This is the responsibility of the information owner.

Operations Security

Terms / Foundations

- Directive control = type of administrative control that is management related. Typically consists of policies and procedures to mandate actions to reduce risk.
- D.A.D. = disclosure (confidentiality attack), alteration (integrity attack), and destruction (availability attack).
- Resources can be sensitive (confidential, secret) and/or critical (operational needs, availability issue)
- Keeping track of the licensing of software is important. This can be an automated or manual process.

- Inventory tracking helps to prevent theft.
- If you hit the emergency power out (EPO) and the servers are still running, it could be that the UPS devices are running.
- Remote maintenance contractor should be given a temporary account.
- The person who installs software should be defined in the policy and should not have programming capabilities.
- Make sure the transportation of media is secure.
- Use shredders to destroy DVDs.
- When you get a new tape system, do not get rid of the old one because they are generally not backward compatible.
- Cold start = complete shutdown, unplug, and restart.
- Secure the role of backup operators because they have full control as well.

Data Recovery Tools

- Backups.
- Electronic vaulting – storing a secondary copy at a remote site.
- Remote journaling – storing on a transaction-by-transaction basis.
- Database shadowing – a copy of your database that may be several stages behind.
- Direct Access Storage Device (DASD).
- RAID:
    - RAID 0 = striping, not reliable, fast.

    - RAID 1 = mirroring; highest availability but greatest cost when scaled.
    - RAID 3=striping & parity drive (byte-level).
    - RAID 4=striping & parity drive (block-level, 512 bytes).
    - RAID 5=striping and parity across all drives.

Network Availability

- Single point of failure – basic availability, high availability, continuous availability (has components to apply planned outages such as upgrades, backups).
- Massive array of inactive disks (MAID) – disks remain dormant.
- Backups – full, differential (since last change), and incremental (since the last backup).
- Tape arrays:
    - RAIT – redundant array of inexpensive tapes (raid for tapes).
    - Network-attached storage (NAS).
    - Serial-advanced technology architecture (S-ATA).
- Online backup:
    - Hierarchical Storage Management (HSM) – combines hard disk w/ jukeboxes. Continuous backup.
    - Storage area network (SAN).

Business Continuity Planning

Terms / Foundation

- PR should be involved in the BCP process.
- Critical business function (CBF): some function without which a business will fail.
- Maximum tolerable downtime (MTD): the amount of time a business can be without some individual CBF.
- The maximum period of disruption: alternative term for MTD.
- Recovery time objective (RTO) The amount of time it will take for a CBF to be restored at a recovery location.
- Recovery point objective (RPO): The amount of data that must be recovered (amount of tolerable data loss).
- Business impact analysis (BIA): an examination of all business functions to find out which of them are CBFs and for each CBF, what their MTD/RPO/RTOs are.
- Keep hard copies of BCP insecure location (like where you store backups).
- The payroll division is not the most critical operation.
- Disaster: any event that causes a CBF to be unavailable for longer than MTD.
- Mirror site = actively running identical processes in parallel (high cost, instant).

- Hot site = fully operational except data/staff (minutes-hours).
- Warm site = partially prepared for operations (Days-weeks).
- Cold site = basic HVAC & connections (weeks-months).
- Mobile site = rent vehicles (trailers, expensive)
- Reciprocal or mutual aid agreements = more than one company share DR responsibilities. Problem: both may be knocked out, no security, asking another side to share disaster; insurance companies don't like it
- Better to have many things wrong with first BCP than no flaws because then you can learn from mistakes
- Types of testing
  - Checklist = give each business a copy of the plan; have them run through a checklist to make sure all relevant points are covered
  - Structured walkthrough = representatives get together in a meeting and review the plan collectively
  - Simulation = practice drill
  - Parallel = an operational test at the alternate site running parallel to production (comparison test)

    - Full interruption = shut down production environment and run a live environment at the alternate site
- If it’s a wide-area disaster, you may have multiple companies competing for a site
- Phases
    - Project Management and Initiation – determine the need for BCP and develop a work plan
    - Business Impact Analysis (BIA) – determine the MTD
    - Recovery Strategy - high-level recovery plan (hot site, cold site decision).
    - Plan Design & Development – specific steps (BCP document).
    - Testing, Maintenance, Awareness, and Training.
- You should tests once a year or whenever there are significant changes.
- Full backup = backing up the entire disk.
- Differential backup = backup data that has changed since the last full backup. This requires you to restore two tapes.
- Incremental backup = backing up the data that has changed since the last backup. This requires you to restore all tapes going back to the last full backup.

Law, Regulations, Compliance, and Investigations

<u>Law</u>

Categories of Law

- Civil law = what is written. Also known as civilist. Civil law systems are like common law systems, but the judges cannot legislate or discard laws as unconstitutional. Civilist judges are more like umpires, deciding which laws apply, whether all procedures were followed, etc.
- Common law = courts. Based on tradition, past practices, legal precedents set by courts through interpretation.
    - Criminal (penal codes). Handled by the judiciary branch.
    - Civil (not the same as a civil law system). Civil law is broken down into contract law and tort law. Handled by the judiciary branch.
    - Tort (negligence, wrong, monetary).
    - Administrative (regulatory agencies). Handled by the executive branch.
- Customary law = tradition
- Religious law = divine. Where the tenets of the religion become the civil and criminal laws of the jurisdiction.
- Mixed law systems = two or more systems.

Intellectual Property Laws

- Three kinds of property:
    - Real Property: land or buildings attached to it.
    - Personal property:
        - Tangible personal property: that which can be touched, moved, etc.
        - Intangible personal property: cannot be touched, such as the value of a shared partnership.
    - Intellectual property: property that comes from a work of art ("art" is the product of a mind).
- Patent = protects against others from practicing the invention covered. Protects idea. Different from country to country (such as durations, starting points, what can or cannot be patented, etc.).
- Trademark™= word, name, symbol, color, sound, product, shape, device to identify goods.
- Copyright© = expression of ideas – original works of authorship.
- Trade secrets = confidential business info that is protected when the owner takes security precautions.

Privacy Laws

- Need for privacy laws:

    - Globalization = distribution of information beyond a single nation (world market).
    - Trans-border data flow = how different nations provide privacy protection of an individual's information.
    - Convergent technologies.
    - Data retrieval advances (vast repositories of personal information exists).
- European Union Principles = information is collected fairly and lawfully only for purposes and only for a reasonable time. If personal information is transmitted to other countries, they must comply with this rule.
- PII = personally identifiable information.

Liability of Corporate Officers

- Due care = act with care of someone with similar training.
- Due diligence = implementing controls, ensuring controls are monitored, etc.
- Negligence = [best practices] - (due care + due diligence).
    - Negligence is often the shortfall between due diligence/care vs. best practices.
- Board of directors can be personally liable.

Investigations

Computer forensics

- A.k.a. Electronic data discovery.
- Digital forensic science (DFS):
    - Media analysis (computer forensics) – physical media.
    - Software analysis (software forensics) – review software for malicious signatures, the identity of the author.
    - Network analysis – network traffic & logs
- Rules of Evidence: electronic evidence is fragile, and you must maintain the integrity of the scene to ensure it is admissible in court.
- Chain of Custody = maintains the integrity of reliability.
- Hearsay rule – An out-of-court statement offered as proof of an assertion.
- Business records exemption: a record used on the normal course of business can be admitted. Computer records may not be hearsay if there was 1) no human intervention; 2) system was operating correctly; and, 3) you can prove no one changed the data.
- Forensic copies:
    - Bit-for-bit – includes hidden & residual data.
    - Ensure integrity with the hash (e.g., MD5, SHA1). Should use duplicate hashes because there are weaknesses

    in hashing algorithms that can make solo hashes risky.
    - Make 2 copies (primary for backup & working for analysis).
    - Zero the media before using it (use proofed media – media verified for being clean).

Incident Response and Handling

- Event: observable occurrence.
- Incident: series of events that impacts business.
- Skills needed:
    - Recognition skills
    - Technical skills
    - Response skills
- Escalation process:
    - Triage: notification and identification.
    - Action/reaction: containment, analysis, tracking.
    - Follow up: repair/recovery, prevention.

Interviewing and Interrogation

- Interviewing: the purpose is to discover information
- Interrogation: the purpose is to obtain evidence for trial.
- Suspect checklist (M.O.M.):

    - Means
    - Opportunity
    - Motives
- Enticement: the act of influencing by exciting hope or desire (admissible).
- Entrapment: the act of a law enforcement officer (LEO) inducing a person to commit a crime (inadmissible in criminal court).
    - There is no such thing as civil entrapment because no, there are no LEOs in civil actions.

Telecommunications, Network, and Internet Security

Foundations

- Packet-switched – statistical TDM (STDM)
- Tree topology used by wireless
- Bluetooth – IEEE 802.15 - uses polling
- FDDI-2 – voice, video, and data
- Maintaining state information – the ability to track that certain packets coming in and going out belong together as part of a session

TCP/IP Model

- Data layer (combines application/presentation/session OSI layers).
- Transport layer (maps to OSI transport layer).

- Internet layer (maps to OSI network layer).
- Network interface layer (maps to data link and physical OSI layers).

OSI Reference Model

- Application:
    - Protocols (FTP, HTTP, IMAP, POP3)
- Presentation:
    - Encryption, compression, format.
- Session:
    - Protocols (RTP, RPC).
- Transport:
    - Protocols (TCP, UDP, TLS).
    - Threats (port scanning - FIN, NULL, XMAS, SYN; denial of service).
- Network
    - Equipment (routers, NAT/PAT, firewalls).
    - Protocols (IP, DHCP, ipv6, ICMP, IGMP, VPN, RIP).
    - Attacks (IP spoofing, SYN floods, source route, smurf, Fraggle).
- Datalink:
    - Unicast/multicast/broadcast.
    - CSMA/CD, CSMA/CA, Token passing.
    - Equipment (switches).
    - Protocols (ARP, PPP).
- Physical:
    - Analog/digital.
    - Topologies (bus, tree, ring, mesh, star).

- Cabling (UTP, coax, fiber, wireless).
- Equipment (patch panel, modem, DSL, hub/repeater, wireless access points).

Wireless Network Standards

- Bluetooth – 2.4Ghz/1Mbps/Frequency Hopping (FHSS).
- 802.11b – 2.4/11/Direct Sequence (DSSS). 11 channels.
- 802.11a – 5/54/Orthogonal Frequency Division Multiplexing (OFDM).
- 802.11g – 2.4/54/OFDM.
- WAP (Int'l standard) & i-Mode.
- 1G wireless – frequency division multiple access (FDMA).
- 2G wireless – time division multiple access (TDMA). GSM & CDMA.
- 2.5G wireless – GPRS, CDMA 2000 1XRTT.
- 3G wireless – Wideband CDMA / UMTS, CDMA 2000 1xdo.
- Mobile phone vulnerabilities – SMS spamming, bluejacking, blue surfing.

Tunneling

- PPTP: uses PPP, can provide some encryption.
- L2F: tunneling, no encryption. Mutual authentication.
- LT2P: PPTP + L2F = L2TP.
- IPSec:

- AH – integrity, origin authentication.
- ESP – encryption – integrity, origin authentication, anti-replay.
- SA – simplex connection (contains IP address, AH/ESP, and SPI).
- SPI – identifies SA.
- Transport adjacency – using the same packet to apply multiple security protocols without invoking tunneling.
- Transport mode – encrypts end-to-end:
    - Iterated tunneling – multiple layers of security protocols through IP tunnels.
- SSH – uses RSA. Does compression, confidentiality, and integrity.

WLAN

- EAP:
    - The 'E' in EAP means extensible (extendable), thus the ability to add two factors to an essentially one factor (PAP/CHAP) system.
    - One factor – EAP-MD5, LEAP, PEAP-MSCHAP, TTLS-MSCHAP, EAP-SIM.
    - Two-factor – EAP-TLS, TTLS w/ OTP, PEAP-GTC.
- Static WEP – same key.
- Dynamic WEP – change keys.
- Temporal Key Integrity Protocol (TKIP) – uses RC4 with 128-bit keys (key + MAC +

Counter changes per packet). Uses a new Message Integrity Code (MIC) called Michael.

- Counter-Mode-CBC-MAC Protocol (CCMP) – uses AES w/128-bit keys.
- Wi-fi Protected Access (WPA):
  - 802.1x or pre-shared key access control.
  - EAP or pre-shared authentication.
  - TKIP (RC4) for encryption.
  - Michael MIC for integrity.
- WPA2 802.11i:
  - 802.1x or pre-shared key access control.
  - EAP or pre-shared authentication.
  - CCMP (AES w/ Counter) for encryption.
  - CCMP (AES CBC-MAC) for integrity.

Remote Access

- PPP:
  - PAP.
  - CHAP.
  - EAP – password, S/Key (MD4 to generate one-time passwords), token card, or digital certificate.
- Radius – UDP, encrypts some.
- TACACS+ - TCP, encrypts all.
- DIAMETER – roaming applications, peer-to-peer:

        - Base protocol – defines message format, transport, error reporting, and security services.
        - Extensions – modules such as Mobile-IP.

Network User Authentication

- LDAP.
- NIS – based on IP address to authenticate clients.
- NIS+ - hierarchical and secure NIS.
- Distributed Computing Environment (DCE).
    - Kerberos.
    - Uses unique universal identifiers instead of user names.
- NTLM.

Perimeter Security

- Bastion host – highly secure system, e.g., application-level gateway.
- Proxy firewalls:
    - Circuit level – doesn't require a proxy for each service. It can require user authentication. E.g., SOCKS. Session layer.
    - Application-level – different proxy for each service. It can require authentication. E.g., Content inspection. Application layer.

- Screened host – uses both packet filtering router and a bastion host.
- Screened subnet – two separate packet filters.
- 3 legged firewall – DMZ.
- Firewall virtualization – use if you need VLANs.

Internet & Web Security Technologies

- SSL:
    - Record Protocol - used to pass messages.
    - Handshake protocol - used to establish an SSL connection.
- Transport Layer Security (TLS) – authentication and protection.
- WTLS – TLS for cell phones, not wireless LANs.
    - Built into the stack, so you just have to turn it on.
    - Encryption & authentication.
    - Encryption stops at the gateway (SSL from the gateway to the webserver) → version 1 only (but nobody uses v2 yet).
- Application layer security protocols
    - Secure remote procedure call (S-RPC).
    - Dnssec.
    - S-HTTP.
    - Electronic payment schemes (SET, Ecash, net cash, Mondex, Cybercash, etc.)

Voice Over IP (VOIP)

- Easier to wiretap.

- DoS attacks on the network can now be applied to phones.
- Need VOIP firewalls and access control systems.
- Some nation’s phone companies are government monopolies, and thus there are laws aimed at protecting incoming voice streams.