DOWNLOAD PDF DISSEMINATING SECURITY UPDATES AT INTERNET SCALE (ADVANCES IN INFORMATION SECURITY)

Chapter 1 : Disseminating Security Updates at Internet Scale : Gerald J. Popek :

The goals of Kluwer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for.

Like traditional crime, terrorism is a local issue and is a responsibility shared among federal, state, and local governments. In the wake of September 11, local law enforcement has taken on a pivotal role in preventing and responding to future incidents of terrorism within the United States. The new policing model for terrorism and homeland security must address the areas of crime prevention, intelligence gathering, and information sharing. This will require a shift in the culture of law enforcement agencies, involving the creation of external partnerships, citizen involvement, problem solving, and the transformation of the organization. In the face of unknown future terrorist threats, however, local law enforcement organizations will have to adapt existing policing strategies to fulfill the requirement of homeland security. Over the years, law enforcement organizations have sought to address the causes and reduce the fear of crime in communities through the creation of effective partnerships with the community and other public and private-sector resources, the application of problem-solving strategies or tactics, and the transformation of agency organization and culture. In the wake of September 11, , local law enforcement agencies throughout the country find themselves struggling to identify their responsibilities and define their future role in the effort to combat terrorism. While some have suggested that community policing can fit into the overall national strategy for homeland security, little research specifically identifies community policing strategies and their direct application to the national strategy for homeland security. Many of the objectives of terrorism prevention parallel current law enforcement policies with respect to local crime issues. Because of these similarities, individual, neighborhood, and community crime-prevention strategies should support law enforcement in the fight against terrorism. In other words, community policing is not in itself a tactic or strategy, but instead a philosophical approach to how policing is conducted. At its core, community-oriented policing is based on law enforcement and the community joining together to identify and address issues of crime and social disorder. In a publication, the U. Department of Justice, Office of Community Oriented Policing discussed a series of community-oriented policing resources and practices that have a direct application to terrorism deterrence and prevention. These include the use of crime mapping with GIS systems, data collection and analysis protocols, and technologies that may be used as platforms for gathering intelligence to assess terrorism vulnerability. In addition, the community partnerships formed by police in the course of community-oriented problem solving provide a ready framework for engaging citizens in helping police to identify possible threats and implement preparedness plans. Scheider, senior analysts at the Office of Community Oriented Policing Services COPS , suggest that community policing could play an integral role in homeland security. They contend that by applying the principles of organizational change, problem solving, and external partnerships, community policing can help police to prepare for and prevent terrorist acts, and respond to the fear such threats engender. Local law enforcement can facilitate information gathering among ethnic or religious community groups with whom police have established a relationship. It will generally be citizens who observe the unusual â€" groups of men living in apartments or motels, or unusual behavior at flight schools â€" in their own community, and could be expected to report such observations to the local police. According to Chapman and Scheider, problem-solving models typically used in community policing are well-suited for preventing and responding to possible terrorist activity. Using existing data sources, agencies can conduct target vulnerability assessments and develop risk-management and crisis plans. The partnerships formed in support of community crime prevention efforts can also provide a framework for engaging citizens to help police identify possible terrorist threats and infrastructure vulnerabilities. Effective community policing involves not only developing partnerships between law enforcement and citizens, however, but also intergovernmental and interagency collaborations with state and federal agencies. These partnerships are essential for the collection and exchange of intelligence, the identification of threats and vulnerabilities, and the sharing of resources in the event of an attack. Problem Solving Problem solving is a broad term that describes the process by which specific issues or concerns are identified and the most appropriate remedies to abate the problem s are identified. By manipulating these factors, people will be less inclined to act in an offensive manner. Such conditions range from the type of individuals involved to the physical environment in which these problems are created. Prior to the advent of community-oriented policing, problem-oriented policing was associated with the decentralization of responsibility and with lateral communication both within and outside the police department. Problem-oriented policing dealt with the conditions that cause a problem; this concept of policing required officers to recognize relationships that lead to crime and disorder and direct their attention to issues of causation. Organizational transformation involves the integration of the community policing philosophy into the mission statement, policies and procedures, performance evaluations and hiring and promotional practices, training programs, and other systems and activities that define organizational culture and activities. Individual officers are presumably the most familiar with their communities and are therefore in the best position to forge close ties with the community and create effective solutions. Community policing emphasizes employee participation; individual officers are given the authority to solve problems and make operational decisions suitable to their assignments. Officers are seen as generalists, not specialists. Adapting Community Policing to Homeland Security Like traditional crime, terrorism is a local crime issue and is a responsibility shared among federal, state, and local governments. Indeed, traditional crime and terrorism are inextricably linked. International and domestic terrorist groups are well-organized and trained, and demonstrate the sophistication of other, traditional organized crime groups. These groups commit ancillary crimes like fraud, money laundering, drug trafficking, and identity theft to provide the resources for their terrorism. The investigative approach to a terrorist event is similar to that of a traditional crime incident. Because of the similarities between traditional crime and terrorism, departments that have already adopted a community policing philosophy should find it a seamless transition to addressing terrorism and terrorism-related crime. Officers should already have the skills to analyze the terrorism problem, perform threat analysis, develop appropriate responses and reflect these efforts in the mission, goals and objectives of the department. Most of the real frontlines of homeland security are outside of Washington D. Likely terrorists are often encountered, and the targets they might attack are protected, by local officials â€” a cop hearing a complaint from a landlord, an airport official who hears about a plane some pilot trainee left on the runway, an FBI agent puzzled by an odd flight school student in Arizona, or an emergency room resident trying to treat patients stricken by an unusual illness. This new role, like the adoption of community policing, will require yet another shift in the culture of law enforcement agencies. Facilitating this shift, however, is the fact that community policing and homeland security have a great deal in common. Both neighborhood crime and terrorism threaten the quality of life in a community and exploit the fear they create. Despite creative ways to stretch public safety budgets, local law enforcement cannot sustain two separate missions of traditional policing and terrorism prevention. Community policing and homeland security can share the same goals and strategies. Creating external partnerships, citizen involvement, problem solving, and transforming the organization to take on a new mission are all key elements of community policing and should be part of a comprehensive homeland security strategy. The lesson learned from fighting traditional crime is that prevention is the most effective approach in dealing with crime, fear, and social disorder. Fighting terrorism is no different. Organizational Transformation The task of a wholesale re-engineering of American local law enforcement toward a counter-terrorism role is complex and unprecedented. Without appropriate and ongoing training of both current and new law enforcement personnel, homeland security will be dismissed as a passing concept instead of a cultural change in law enforcement strategy. There are a number of community policing practices that can support efforts in homeland security. These practices include adopting the philosophy organization-wide, decentralizing decision-making and accountability, fixing geographic and general responsibilities and utilizing volunteer resources. Local law enforcement officers are most likely to come into contact with individuals who are either directly or indirectly involved in terrorist activities and are certain to be the first responders to any attack. Empowering officers at lower levels with greater decision-making authority and responsibility for important decisions could be valuable in a crisis. During a terrorist event, there may be little time for decisions to move up the chain of command. Officers who are accustomed to making decisions and retaining authority may be better prepared to respond quickly and decisively to any event. In terms of prevention, developing a flat organizational structure can help lower-level officers feel free to pursue leads regarding possible terrorist activity. In addition, officers who work in a fixed geographic area for an extended period are more likely to develop specific intelligence that may be a vital part of counter-terrorism efforts. Training Local agencies will need to expand beyond the rudimentary aspects of law enforcement training such as firearms, driving, unarmed defense and criminal law into one that emphasizes an analytical preventative approach. While law enforcement must continue to train for their roles as first responders in post-incident management and investigation, police must receive training and education in: Understanding the nature, dynamics, and operations of international terrorist groups that may operate in or against the United States, and how that translates into more effective patrol and investigative functions; Understanding the locations, movements, and plans of international terrorist cells that live and work in local communities; Gathering and analyzing intelligence on potential terrorist activities; Conducting threat assessments; Conducting inquiries and investigations into potential terrorists while safeguarding the constitutional rights of all people in the United States. Most local law enforcement officers have never been in the intelligence business and therefore may not know precisely what information they should look at as indicative of terrorist activity or that may have value within a larger intelligence context. These signs are not necessarily obvious, but rather subtle, and would be discernible to a regular patrol officer or detective with proper training. Officers or detectives may have valuable information without even knowing it and may not know to share the information because they have never had adequate terrorism intelligence training. Another area of training that law enforcement must commit to is public education. Although the majority of communities will never be impacted by a terrorist event, the threat of potential terrorist attacks can create fear and undermine the sense of community safety. It will therefore be critical that police take a leadership role in maintaining community confidence. This can be done by educating the public as to the nature of threats and actively responding to specific community concerns. For the public to respond to an alert, it needs to know what to watch for. Educating the public also garners support for government action in a crisis. Moreover, citizens educated about potential threats can assist law enforcement during alerts. The public would know what to look for, what to do, and how to respond. Leadership is required and rewarded at every level; supervisors and officers are held accountable for decisions and the effects of their efforts at solving problems. Empowering officers at the lower levels will allow them the freedom to pursue leads or suspected terrorist activity, or to identify possible terrorist vulnerabilities within the community. Fixed Geographic Accountability and Generalist Responsibilities In community policing, most staffing, supervision, deployment, and tactical decision-making are geographically based. Personnel are assigned to fixed geographic areas for extended periods of time in order to foster communication and partnerships between individual officers and their community. Having fixed-geographic responsibility allows officers to develop more productive relationships with members of their community and, as a result, officers should be more attuned to rising levels of community concern and fear. By virtue of these relationships, officers should be in a position to respond effectively to those needs and concerns. Community policing engenders trust and increases satisfaction among community members and police, which in periods of heightened unrest or crisis can translate to dealing more effectively with community fear. This network of volunteer efforts uses the foundations already established by law enforcement in order to prepare local communities to respond effectively to the threats of terrorism and crime. Community policing encourages the use of non-law enforcement resources within a law enforcement agency such as volunteerism, which involves active citizen participation with their law enforcement agency. Volunteer efforts can help free up officer time, and provide an effective channel for citizen input. It has long been recognized that many of the basic functions within a law enforcement agency can be accomplished by other than sworn deputies or civilian employees. Volunteer efforts can help free up officer time, and allow sworn personnel to be more proactive and prevention-oriented. In many jurisdictions around the country, citizens who have the time to volunteer in the community have offered their services to law enforcement agencies, freeing up law enforcement personnel to spend more time in a crime reduction role. In fact, Neighborhood Watch has been an integral component of the community policing philosophy virtually since its inception. Neighborhood Watch This crime prevention program, which has a thirty-year history, engages volunteer citizen action to enhance security within local communities by encouraging citizens to report suspicious activity in their immediate neighborhoods. In the aftermath of September 11, , the need for strengthening and securing our communities has become even more critical, and Neighborhood Watch groups have taken on greater significance. In addition to serving a crime prevention role, Neighborhood Watch can also be used as the basis for bringing neighborhood residents together to focus on disaster preparedness as well as terrorism awareness, to focus on evacuation drills and exercises, and even to organize group training, such as the Community Emergency Response Team CERT training. Since September 11, , the demands on state and local law enforcement have increased dramatically. As a result, already-limited resources are being stretched farther at a time when our country needs every available officer out on the beat. The program provides resources to assist local law enforcement officials by incorporating community volunteers into the activities of the law enforcement agency and by using best practices to help state and local law enforcement design strategies to recruit, train, and utilize citizen volunteers in their departments. President Bush has proposed a three-fold increase, to ,, of the number of citizens enrolled in CERT. Since its move into Citizen Corps, the program has added a new module that addresses terrorism preparedness. When emergencies happen, CERT members can give critical support to first responders, provide immediate assistance to victims, and organize spontaneous volunteers at a disaster site. CERT members can also help with non-emergency projects that help improve the safety of the community.

Chapter 2 : Disseminating Security Updates at Internet Scale : Jun Li :

Disseminating Security Updates at Internet Scale will be helpful to those trying to design peer systems at large scale when security is a concern, since many of the.

Job Rotation[edit] Job Rotation is an approach to management development where an individual is moved through a schedule of assignments designed to give him or her a breath of exposure to the entire operation. Job rotation is also practiced to allow qualified employees to gain more insights into the processes of a company and to increase job satisfaction through job variation. Separation of Duties[edit] Separation of duties SoD is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties or, in the political realm, separation of powers. Without those few and far between expert level techs who can have or get the administration rights to view all aspects of any given production process it will be nearly impossible to determine the underlying cause and can lead to outrageous decisions as to what the problem must of been. Or nobody realizing the automated software machine was running into RAM issues because every automated job was set to auto start at exactly 6: With the concept of SoD, business critical duties can be categorized into four types of functions, authorization, custody, record keeping and reconciliation. In a perfect system, no one person should handle more than one type of function. In information systems, segregation of duties helps reduce the potential damage from the actions of one person. IS or end-user department should be organized in a way to achieve adequate separation of duties Control Mechanisms to enforce SoD There are several control mechanisms that can help to enforce the segregation of duties: Audit trails enable IT managers or Auditors to recreate the actual transaction flow from the point of origination to its existence on an updated file. Good audit trails should be enabled to provide information on who initiated the transaction, the time of day and date of entry, the type of entry, what fields of information it contained, and what files it updated. Reconciliation of applications and an independent verification process is ultimately the responsibility of users, which can be used to increase the level of confidence that an application ran successfully. Exception reports are handled at supervisory level, backed up by evidence noting that exceptions are handled properly and in timely fashion. A signature of the person who prepares the report is normally required. Manual or automated system or application transaction logs should be maintained, which record all processed system commands or application transactions. Supervisory review should be performed through observation and inquiry and the trust built with directory one-level up managers. To compensate repeated mistakes or intentional failures by following a prescribed procedure, independent reviews are recommended. Such reviews can help detect errors and irregularities but are usually expensive can raise questions as to how much can an outside independent review once a quarter know about your processes compared to people within and what level of trust can be built with those independent reviewers. Least Privilege Need to Know [edit] Introduction The principle of least privilege, also known as the principle of minimal privilege or just least privilege, requires that in a particular abstraction layer of a computing environment every module such as a process, a user or a program on the basis of the layer we are considering must be able to access only such information and resources that are necessary to its legitimate purpose. This principle is a useful security tool, but it has never been successful at enforcing high assurance security on a system. Benefits Better system stability. When code is limited in the scope of changes it can make to a system, it is easier to test its possible actions and interactions with other applications. In practice for example, applications running with restricted rights will not have access to perform operations that could crash a machine, or adversely affect other applications running on the same system. When code is limited in the system-wide actions it may perform, vulnerabilities in one application cannot be used to exploit the rest of the machine. In general, the fewer privileges an application requires the easier it is to deploy within a larger environment. This usually results from the first two benefits, applications that install device drivers or require elevated security privileges typically have addition steps involved in their deployment, for example on

Windows a solution with no device drivers can be run directly with no installation, while device drivers must be installed separately using the Windows installer service in order to grant the driver elevated privileges Mandatory Vacations[edit] Mandatory vacations of one to two weeks are used to audit and verify the work tasks and privileges of employees. This often results in easy detection of abuse, fraud, or negligence. Job Position Sensitivity[edit] Security Roles and Responsibilities[edit] Levels of Responsibilities[edit] Senior management and other levels of management understand the vision of the company, the business goals, and the objectives. Functional management, whose members understand how their individual departments work, what roles individuals play within the company, and how security affects their department directly. Operational managers and staff. These layers are closer to the actual operations of the company. They know detailed information about the technical and procedural requirements, the systems, and how the systems are used. The employees at these layers understand how security mechanisms integrate into systems, how to configure them, and how they affect daily productivity. Classification of Roles and their Responsibilities[edit] Data Owner The data owner information owner is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of a specific subset of information. The data owner decides upon the classification of the data that he is responsible for and alters that classification if the business needs arise. This person is also responsible for ensuring that the necessary security controls are in place, ensuring that proper access rights are being used, defining security requirements per classification and backup requirements, approving any disclosure activities, and defining user access criteria. The data owner approves access requests or may choose to delegate this function to business unit managers. And it is the data owner who will deal with security violations pertaining to the data he is responsible for protecting. The data owner, who obviously has enough on his plate, delegates responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian. Data Custodian The data custodian information custodian is responsible for maintaining and protecting the data. System Owner The system owner is responsible for one or more systems, each of which may hold and process data owned by different data owners. A system owner is responsible for integrating security considerations into application and system purchasing decisions and development projects. The system owner is responsible for ensuring that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on. This role needs to ensure that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner. The security administrator role needs to make sure that access rights that are given to users support the policies and data owner directives. Security Analyst This role works at a higher, more strategic level than the previously described roles and helps to develop policies, standards, and guidelines and set various baselines. Whereas the previous roles are "in the weeds" and focusing on their pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure that the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level. Application Owner An application owner, usually the business unit managers, are responsible for dictating who can and cannot access their applications, like the accounting software, software for testing and development etc. Change Control Analyst The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role needs to make sure that the change will not introduce any vulnerability, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Data Analyst The data analyst is responsible for ensuring that data is stored in a way that makes the most sense to the company and the individuals who need to access and work with it. The data analyst role may be responsible for architecting a new system that will hold company information or advising in the purchase of a product that will do this. Process Owner Security should be considered and treated like just another business process. The process owner is responsible for properly defining, improving upon, and monitoring these processes. A process owner is not necessarily tied to one business unit or application. Complex processes involve a lot of variables that can span across different departments, technologies, and data types. Solution Provider This role is called upon when a business has a problem or requires that a process be improved upon. User The user is any individual who routinely uses the data for work-related tasks. Product Line Manager Responsible for explaining business requirements to vendors and wading through their rhetoric to see if the product is right for the company Responsible for ensuring compliance to license agreements Responsible for translating business requirements into objectives and specifications for the developer of a product or solution Decides if his company really needs to upgrade their current systems This role must understand business drivers, business processes, and the technology that is required to support them. The product line manager evaluates different products in the market, works with vendors, understands different options a company can take, and advises management and business units on the proper solutions that are needed to meet their goals.

Chapter 3 : Top 5 emerging information security technologies

Disseminating Security Updates at Internet Scale presents experimental measurements of a prototype implementation of "Revere" gathered using a large-scale oriented approach. These measurements suggest that "Revere" can deliver security updates at the required scale, speed and resiliency for a reasonable cost.

As soon as the white hats counter one form of black-hat malicious behavior, another malevolent form rears its ugly head. How can the playing field be tilted in favor of the infosec warriors? Here are five emerging security technologies that may be able to do that. Application Security Research Update: Hardware authentication The inadequacies of usernames and passwords are well known. Clearly, a more secure form of authentication is needed. Intel is moving in that direction with the Authenticate solution in its new, sixth-generation Core vPro processor. Intel has built on previous efforts to dedicate a portion of the chipset for security functions to make a device part of the authentication process. Good authentication requires three things from users: In the case of Authenticate, the device becomes the what-you-have. However, Crawford noted, "The most immediate application for the technology is for authenticating an endpoint in a traditional IT environment â€" laptops, desktops, and mobile devices using Intel chipsets. The technology uses big data analytics to identify anomalous behavior by a user. Data loss prevention A key to data loss prevention is technologies such as encryption and tokenization. They can protect data down to field and subfield level, which can benefit an enterprise in a number of ways: Cyber-attackers cannot monetize data in the event of a successful breach. Data can be securely moved and used across the extended enterprise â€" business processes and analytics can be performed on the data in its protected form, dramatically reducing exposure and risk. The enterprise can be greatly aided in compliance to data privacy and security regulations for protection of payment card information PCI , personally identifiable information PII and protected health information PHI. Deep learning Deep learning encompasses a number of technologies, such as artificial intelligence and machine learning. Like user behavior analytics, deep learning focuses on anomalous behavior. For example, a data center, as an entity, can behave a certain way, similar to a user. Crawford said he expects investments in deep learning for security purposes to continue. He added, however, that "the challenge for enterprises is there are a lot of companies coming to market with similar approaches for the same problem. Differentiating distinctions from one vendor to another is going to be a major challenge for enterprises in the coming year and beyond. The cloud "The cloud is going to have a transformative impact on the security technology industry generally," Crawford said. He explained that as more organizations use the cloud for what has traditionally been the domain of on-premises IT, more approaches to security that are born in and for the cloud will appear. On-premises techniques will be transitioned to the cloud. Things such as virtualized security hardware, virtualized firewalls, and virtualized intrusion detection and prevention systems. But that will be an intermediate stage. These five should help out the infosec warriors get the upperhand. Which technologies do you suggest will move the needle on information security? Weigh in via the comments below.

Chapter 4 : Update your browser to access the Norton website

Disseminating Security Updates at Internet Scale describes a new system, "Revere", that addresses these problems. "Revere" builds large-scale, self-organizing and resilient overlay networks on top of the Internet to push security updates from dissemination centers to individual nodes.

Additional Information In lieu of an abstract, here is a brief excerpt of the content: However, today, attackers have the upper hand. In this chapter, I discuss the security properties needed, and some key strategies that may have the potential to level the playing field between attackers and defenders. These research strategies were developed at the National Cyber Leap Year summit, with experts from industry, academia , and government working collaboratively. These broad research thrusts can be interpreted at different levels of the system, and in different application domains. Because a promising direction explored at the summit is the use of hardware architecture to enhance security, I provide a hardware-enhanced interpretation of the proposed research thrusts, with the goal of illustrating how new security features can be built into future commodity computers to improve system security. The goal is to be able to ensure essential security features for critical tasks, even in the presence of malware and software vulnerabilities in the system, and users who are not Improving Cyber Security Ruby B. Lee 38 Ruby B. Feasibility examples are given to show how new hardware security features can help improve software security and also how hardware itself can be designed to be more trustworthy. These examples illustrate that by rethinking the fundamental design of computers with security as one of the key requirements, we can design future secure, trustworthy computers without necessarily sacrificing performance and other goals. Cyber Security Today In its early days, the Internet was used as a means of enhancing research among collaborating scientists. The success of this design can be seen today in the various applications built on top of the Internet, such as the World Wide Web, search, web mail, e-commerce, e-banking, and social network applications. Today, our social lives, our economic competitiveness , our national security, and in fact all aspects of our lives depend on the correct functioning and ubiquitous availability of the Internet and wireless networks. This dependence on the Internet and on cyberspace transactions is increasing at the same time cyber attacks are escalating. The technologies that make up cyberspace were not designed with security in mind. Internet protocols were designed for friendly parties to communicate and collaborate with each otherâ€”they were not designed with malicious adversaries in mind. Similarly, computer technology, both hardware and software, was not designed with attackers in mind. Hence, it should not be surprising that the basic network, soft1. Improving Cyber Security 39 ware, and hardware technologies underlying cyberspace are full of security vulnerabilities that can be exploited by malicious parties. In addition, attackers only need to find one path into the system to infiltrate it, whereas defenders have to defend on all fronts. In a DDoS attack, an army of zombies also called a botnet is harnessed to attack a primary victim, which could be a website, computer, or network see Figure 1a. Such stealthy infiltration of computers and installation of zombie programs can be done months before an actual DDoS attack is launched. They are possible due to security vulnerabilities, most often in the software, that can be exploited by an attacker to infiltrate a computer and silently install a zombie program without being detected. You are not currently authenticated. View freely available titles:

Chapter 5 : Security and protection system | personal and property protection | www.nxgvision.com

Revere system builds large-scale, self-organizing and resilient overlay networks on top of the Internet to push security updates from dissemination centers to individual nodes.

Security is another important database issue. Data residing on a computer is under threat of being stolen, destroyed, or modified maliciously. This is true whenever the computer is accessible to multiple users but is particularly significant when the computer is accessible over aâ€¦ Development of security systems. The origins of security systems are obscure, but techniques for protecting the household, such as the use of locks and barred windows, are very ancient. As civilizations developed, the distinction between passive and active security was recognized, and responsibility for active security measures was vested in police and fire-fighting agencies. By the midth century, private organizations such as those of Philip Sorensen in Sweden and Allan Pinkerton in the United States had also begun to build efficient large-scale security services. Until the advent of collective bargaining in the United States, strikebreaking was also a prime concern. The Sorensen organization, in contrast, moved toward a loss-control service for industry. It provided personnel trained to prevent and deal with losses from crime, fire, accident , and flood and established the pattern for security services in the United Kingdom and elsewhere in western Europe. After World War II much of this apparatus was retained as a result of international tensions and defense-production programs and became part of an increasingly professionalized complex of security functions. The development and diffusion of security systems and hardware in various parts of the world has been an uneven process. In relatively underdeveloped countries, or the underdeveloped parts of recently industrializing countries, security technology generally exists in rudimentary form, such as barred windows, locks, and elementary personnel security measures. In many such regions, however, facilities of large international corporations and sensitive government installations employ sophisticated equipment and techniques. Since the s, crime-related security systems have grown especially rapidly in most countries. Among contributing factors have been the increase in number of security-sensitive businesses; development of new security functions, such as protection of proprietary information; increasing computerization of sensitive information subject to unique vulnerabilities; improved reporting of crime and consequent wider awareness; and the need in many countries for security against violent demonstrations, bombings, and hijackings. Security systems are becoming increasingly automated, particularly in sensing and communicating hazards and vulnerabilities. This situation is true in both crime-related applications, such as intrusion-detection devices, and fire-protection alarm and response extinguishing systems. Advances in miniaturization and electronics are reflected in security equipment that is smaller, more reliable, and more easily installed and maintained. Types of security systems. Security systems can be classified by type of production enterprise, such as industrial, retail commercial , governmental, government contractor, or hospital; by type of organization, such as contract security or proprietary; by type of security process, such as personnel or physical security; or by type of security function or emphasis, such as plant protection variously defined , theft control, fire protection, accident prevention, protection of sensitive national security or business proprietary information. Some of these categories obviously overlap. Security for small businesses constitutes a special situation. Because small firms cannot afford specialized proprietary security staffs, measures must be incorporated into regular routines and staff training or be purchased from outside organizations. Theft, both internal and external, is a prime concern. Residential security constitutes another special category. Sizable housing or apartment complexes, especially if under one management, can employ sophisticated security measures, including, for example, closed-circuit television monitoring of elevators and hallways and trained security guards. Relatively simple equipment for houses or small apartment buildings, as, for example, exterior lighting and alarms, is increasingly used. Some neighbourhoods of large cities cooperatively employ patrol services or organize resident volunteer patrols. Some of the most effective advances in security technologies during the past few decades have been in the area of physical securityâ€”i.

Physical security has two main components: A building can be designed for security by such means as planning and limiting the number and location of entrances and by careful attention to exits, traffic patterns, and loading docks. Equipment and devices may be classified in various categories depending on the criteria used. If the criterion is purpose, some of the principal categories are record containers, including safes and files; communications, such as two-way radios and scrambler telephones; identification, including badges and automatic access-control systems requiring the use of a code; investigation and detection e. A classification system based on process results in another set of categories. Examples include perimeter barriers e. Advances in security equipment technology have been numerous. A major part of security programs consists of measures designed to recruit and effectively use trustworthy personnel. Thus, the dossier and computerized national data banks exemplify a response by a society in which great geographic mobility necessitates record keeping as a basis for judgments. Another technique is the polygraph, or lie-detector, examination. Research has also been directed to the possible capabilities and limitations of pencil-and-paper psychological tests and stress interviews. In addition to selection techniques there are other measures designed to keep personnel trustworthy after they have been brought into the systemâ€”for example, employee indoctrination programs and vulnerability testing. Systems and procedures constitute another area of the personnel-administration approach to security. It is possible to devise work methods and management controls in such a way that security is one of the values sought along with maximizing productivity and minimizing cost. Examples include the use of automated record-keeping systems, the use of forms and reports periodically checked against physical inventories, and the application of the principle of dual responsibility, whereby work is so subdivided that the work of one employee checks the accuracy of the work of another. Because control systems are not self-administering, they must be periodically tested and policed. Guard-force training, supervision, and motivation are other important aspects of the personnel-administration approach to security. The use of operational personnel to attain security objectives is still another. Examples include engineers, production workers, and clerical staff applying government security regulations for the safeguarding of classified information, and salespeople cooperating with security staff in the detection of shoplifters. The cooperation of operational personnel to attain security objectives along with production objectives demands an interplay between knowledgeable training and communication programs, supervision, employee motivation, and management example. The personnel-relations approach implicit in much of the above recognizes that the attitudes of rank-and-file employees and the social climate that they create can either be conducive to security or constitute its greatest enemy. Therefore, if security programs are to be successful, they must be carried out in a context of considerable understanding and cooperation of virtually the entire work force. The security program is apt to be only as good as the overall pattern and climate of social relations and loyalties of workers and executives of all ranks. Learn More in these related Britannica articles:

Chapter 6 : CiNii å›³æ›¸ - Disseminating security updates at Internet scale

UNIVERSITY OF CALIFORNIA Los Angeles Revereâ€” Disseminating Security Updates at Internet Scale A dissertation submitted in partial satisfaction of the requirements for the degree.

Chapter 7 : Cass County Today â€“ A Service of KAQC TV

Disseminating Security Updates at Internet Scale by Gerald J. Popek, , available at Book Depository with free delivery worldwide.

Chapter 8 : dblp: Advances in Information Security

Revere provides a service for disseminating security updates at Internet scale. To understand how effective Revere is in *providing this service, the characteristics of the dissemination must be.*

Chapter 9 : Project MUSE - Advances in Cyber Security

Disseminating Security Updates at Internet Scale will be helpful to those trying to design peer systems at large scale when security is a concern, since many of the issues faced by these designs are also faced by "Revere".