By Greg Hill, FreshBaked.com®

Within businesses, security issues, and their consequences for the general public, saturate the news. With large organizations, even those with substantial budgets, well financed IT/IS departments and resources dedicated to system security, often do not do an appreciably better job than smaller enterprises with fewer resources and either no plan or a largely ineffective one.

Most recently eBay and Target are alarming examples, and although those garner the most attention, as destructive both financially and to public peace of mind, the area of greatest concern is largely overlooked. These are the entities Homeland Security defines as Critical Infrastructure, "the backbone of our nation's economy, security and health."

This paper will examine the threats to which these types of organizations are vulnerable, as well as the common mistakes being made that increase their susceptibility to the risks. Poorly planned and ineffectively implemented security measures may result in unintended consequences such as the loss of productivity and business confidentiality will also be examined. Finally, a template for developing an effective security plan will be included.

Contents

The Need for Effective Security

Security is not isolated to technical/computer areas of an organization, but rather is a model to be embraced as an organization-wide managerial concept not something left only to technicians.

Security is often divided into intuitive categories such as physical security and information or cybersecurity, but in today's world, they are too closely integrated and overlapping to separate and must be managed as a single initiative to effectively keep the enterprise safe from harm.

Physical security, of course, is concerned with the protection of people and things, primarily employees and physical assets, and utilizes methods that most people are familiar with, such as security guards, door locks, fences, etc.

Cybersecurity or Information Security, on the other hand, protects electronic information, which is stored on the organization's computers, networks, and other devices. For the sake of simplicity and in keeping with Homeland Security and National Institute of Standards and Technology (NIST), we will use cybersecurity as the descriptive term.

Since these two areas of security overlap the effectiveness of one depends on the other. Example: Electronic information is contained on physical machinery, like computers, which must be protected from physical as well as cyber access. Physical security also depends on the enterprise network to provide the means to conduct and monitor its operations using cameras, software and various detection devices such as heat and motion detectors, time locks, alarms, VOIP telephones, etc.

While acknowledging that physical security is a critical component of the overall security plan, it will not be fully considered within the scope of this document other than to assume that the security of the physical devices is assured.

Cybersecurity is a vague and all encompassing term and necessitates a detailed plan in order to be effectively implemented. But before a plan can be devised, the organization needs to evaluate the risks and establish goals by which to judge the success or failure of each facet of the plan. This is the area that represents a particular challenge to small and medium-sized organizations, because their lack of resources may contribute to a lack of awareness, both of what should be protected and what are the most effective methods.

There may even be a common misconception among smaller entities that they do not need security, because they are too small or too hidden to attract the attention of the cyber criminals. This form of "Security by Obscurity" is not valid for a number of reasons, including that predatory entities use automated approaches that look for targets, and seldom have the means or inclination to grade them based on size.

Over a decade of data collected by Verizon in its Data Breach Investigation Report indicates that cyber criminals are concentrating on smaller businesses, possibly because their defenses are less rigorous. All organizations should endeavor to isolate what should not be accessible to the public, reducing their exposure whenever possible. There is a saying in the security trade that there are only two kinds of organizations: "…those that have experienced a breach, and those who are simply not aware that they have." (High, 2014)

Complicating planning for effective security is the certainty that there is no possibility of a 100% effective plan and that even companies that spend millions of dollars on sophisticated models still suffer embarrassing public security breaches. This is the reason behind developing a list of risks, weighted by importance to the organization. In other words, according to the Global State of Information Security® Survey 2014 (GSISS-2014):

"While information security risks have dramatically evolved, security strategies—typically compliance-based and perimeter-oriented—have not kept pace. In other words, most organizations are now defending yesterday, even as their adversaries look to exploit the vulnerabilities of tomorrow.

Consequently, sophisticated intruders are bypassing perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. Many use well-researched phishing exploits that target top executives.

Similarly, the attack surface—partners, suppliers, customers, and others—has expanded as an ever-greater volume of data flows through multiple channels. The result? Safeguarding all data at an equally high level is no longer practical." (Cooper, 2014)

If you can't protect everything equally, you must protect those items that represent the highest risk.

One of the largest threats to all organizations is the Data Breach[1]. Verizon's 2014 Data Breach Investigations Report narrows down the possible threats by revealing that 92% of all of the breaches investigated fell into nine patterns (Cooper, 2014):

1. Point of Sale Intrusions
2. Web App Attacks
3. Insider and Privilege Misuse

[1] "A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so." Wikipedia, http://en.wikipedia.org/wiki/Data_breach
A security breach is "An act from outside an organization that bypasses or contravenes security policies, practices, or procedures. A similar internal act is called security violation."
The Business Dictionary, http://www.businessdictionary.com/definition/security-breach.html#ixzz32IsO7ttE

4. Theft and Loss
5. Miscellaneous Errors
6. Crimeware
7. Payment card skimmers
8. Denial of Service
9. Cyber Espionage

Of these nine patterns, only three may be effectively defended with physical security: Insider and Privilege Misuse, Theft and Loss, and Payment card skimmers. The others are primarily the result of cyber attacks, i.e. using software, computers and networks without physical access.

Verizon also broke down the frequency of breaches by industry, which serves as an excellent starting point for planners to prioritize risks. For example, Retailers have the most to fear from POS Intrusions (31% of breaches) and Denial of Service (DoS) attacks (33%). Public organization risks were concentrated in Miscellaneous Errors (34%), Insider Misuse (24%), Crimeware (21%), and Theft and Loss (19%).

One group, the Accommodation industry has a very clear objective for their security planning because POS Intrusions accounted for 75% of breaches. Those interested in evaluating the effectiveness of security plans should begin with a thorough reading of the Verizon DBIR report available at http://www.verizonenterprise.com/DBIR/2014/.

Data breaches are not the only vulnerability faced by organizations, but they may be the most expensive, frequently threatening their very existence. The United States Congress has failed to establish automatic penalties for data breaches after several attempts, but they still have wide-reaching costs, estimated by the latest Ponemon/IBM study at $5.9 million dollars per occurrence (Institute, 2014), not including other costs such as lost business and goodwill, which may be even more damaging.

Data breaches involving medical records do have mandatory disclosure and notification rules, administered by the Health Information Portability and Accountability Act (HIPAA) and the Federal Trade Commission (FTC), which order disclosure to affected persons, the media and government with the possibility of fines for breaches involving 500 or more people. (Commission, 2009)

Security breaches that do not involve data are frequently not widely publicized, but are at least as dangerous and must be protected against as diligently. According to PC World, High profile areas of concern for 2014 include Mobile malware, the Internet of Things (IoT), Virtual currencies, and Windows XP. (Bradley, 2014)

Mobile malware may prove to be the largest threat in the coming years, due to the obvious massive proliferation of Smartphones and tablets in the workplace, and the less apparent surreptitious spread of mobile malware, as described in this passage from PC World:

> "James Lyne, global head of security research for Sophos, notes that mobile malware is adapting and evolving faster than security tools can learn to detect and evade the threats. Variants are adopting tactics from PC malware—employing encrypted command and control servers, and polymorphism, among other techniques. The perfect storm is on its way."

The Internet of Things (IoT), called by many other similar names by vendors marketing connected products, represents a growing vulnerability for individuals and enterprises. The IoT involves installing smart chips into consumer and commercial products, giving them an address, and connecting them to the Internet, from which they can be controlled.

There is a great deal of concern today about government agencies and/or criminals monitoring the general public through their phones and computers, including spying through cameras built-in to these devices. With the IoT, this capability expands to automobiles, appliances, wristwatches, health trackers, bicycles, and eventually nearly any item that is large enough to contain a battery and a computer chip. There are chips in lawnmowers, golf bags, and even some light bulbs – with no end in sight.

This brings up at least two new vulnerabilities to be included in the Security Plan: first, awareness of everything that can be connected to the Internet, because it may be used to break into the network in addition to providing information to the outside world. Secondly, the need for Internet addresses caused by the IoT has outstripped the current system, IP V4, and has resulted in a new addressing system, IP V6. The new system requires new operational and security software to be written. Any new system is less secure than a mature system where the holes have been plugged.

PCWorld's other 2014 high risk categories included Virtual Currencies and Windows XP exploits. Since Virtual Currencies are not in widespread use, they do not pose a significant risk to most organizations. Windows XP problems should pass quickly as hardware is upgraded. But, there will always be another major software package that is no longer being supported by its manufacturer and any Security Plan developed should account for the expiration and replacement of software.

Other Security Breaches must also be considered by all organizations. AOL, for example reported a recent incident where hackers got into their system in order to send phishing[2] emails (Blair, 2014). Phishing is already highly effective, with an 8% success rate according to the Verizon DBIR survey, and phishing attacks from recognized email addresses have the potential to be even more effective.

[2] **Phishing** is the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Wikipedia, http://en.wikipedia.org/wiki/Phishing.

Critical Infrastructure organizations[3] may have additional threats due to their widespread dependence on SCADA (Supervisory Control and Data Acquisition) systems to control plant equipment. According to a report by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), reported incidents have increased from nine in 2009 to 256 in 2013. (Wide-Area Situational Awareness for Critical Infrastructure Protection, 2013) (ICS-CERT, 2014) The January – April 2014 issue of the ICS-CERT Monitor starts with the following chilling warning:

> "Is your control system accessible directly from the Internet? Do you use remote access features to log into your control system network? Are you unsure of the security measures that protect your remote access services? If your answer was yes to any or all these questions, you are at increased risk of cyber attacks including scanning, probes, brute force attempts and unauthorized access to your control environment."

This statement is particularly important because many of these organizations do not include the SCADA (a.k.a. "Control") networks in their security plans because they are physically isolated from the Internet-facing business network (a.k.a. the "Dirty" network). In many cases, this is a false assumption, because doorways are open into the SCADA network and security planners may not be aware.

These vulnerabilities include the (assumed) secure connection between the Control and Dirty network which may be vulnerable to exploitation by hacking or social engineering/phishing4. Another source of entry into the Control network enumerated by ICS-CERT is SCADA-enabled devices that are unintentionally connected to the Internet by Wi-Fi, cellular, telephony, or other communications protocols. These connections may be intended for other purposes, such as status monitoring or meter reading, but may be exploitable using publicly available software or commands.

Each one of the threats above represents serious risks to most industry types. But organizations should not treat risks equally when forming their security plan, but should instead use the universal formula: R = T * V, or Risk = Threat times Vulnerability (to that threat) (Institute, 2014). In short, no matter how serious a threat is, if the vulnerability is low the risk is reduced or non-existent, and security and mitigation

[3] Critical Infrastructure (CI) organizations are defined as assets that are essential for the functioning of a society and economy. Sectors of CI identified by the Homeland Security agency of the U.S. Government are Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, (Nuclear Reactors, Materials, and Waste Transportation Systems), Water and Wastewater Systems. (ICS-CERT, 2014)

[4] Social engineering would be getting the passwords and access information from an individual by using persuasive social techniques. Phishing is acquiring the same credentials by posing as authorities or administrators and tricking employees into voluntarily disclosing the information.

procedures may be a waste of resources that could better be devoted to more elevated risks.

Every organization with stored information needs a security plan, because even if they do not store any sensitive or personal information, they still store information that is required to run the business and would be expensive to replace.

The small to medium-sized businesses all need a security plan, even if it is just a few pages specifying policies and guidelines to protect critical information. And, since security plans do not write themselves, each business must have a Security Officer (SO), preferably a full-time dedicated position, but in the smallest of businesses, a manager must also serve in this role.

Paragraphs 18 and 19 of the Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD7), dated December 17, 2013 designates which Federal Agencies will watch over each Critical Infrastructure segment, and what their roles and responsibilities will be:

18. *Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, there are designated Sector-Specific Agencies, including:*
    1. *Department of Agriculture -- agriculture, food (meat, poultry, egg products);*
    2. *Health and Human Services -- public health, healthcare, and food (other than meat, poultry, egg products);*
    3. *Environmental Protection Agency -- drinking water and water treatment systems;*
    4. *Department of Energy -- energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities;*
    5. *Department of the Treasury -- banking and finance;*
    6. *Department of the Interior -- national monuments and icons; and*
    7. *Department of Defense -- defense industrial base.*
19. *In accordance with guidance provided by the Secretary, Sector-Specific Agencies shall:*
    1. *collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;*
    2. *conduct or facilitate vulnerability assessments of the sector; and*
    3. *encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.*

Because of this directive, and others from the Federal Government, a number of risk management strategy documents have been developed based on input from some of

the certification organizations above as well as noted experts in the field of security in both the public and private sector.

The proposed formula for forming a Security Plan is largely drawn from this guidance as it applies to Critical Infrastructure organizations, which is intended to develop the most complete risk reduction strategy for these types of entities. Organizations with lower overall risk profiles, i.e. those not designated as Critical Infrastructure, should view this as a "worst-case scenario" and adjust as they see fit, while being exposed to more extensive measures should it become necessary to implement them in the future.

The primary Federal documents referenced in this presentation are the Framework for Improving Critical Infrastructure Cybersecurity and the National Infrastructure Protection Plan (NIPP) detailed in the document NIPP 2013 – Partnering for Critical Infrastructure Security and Resilience. (Technology, 2014) (2013)

This document was developed with "…the active participation of the critical infrastructure community, including private industry; public and private sector owners and operators; State, local, tribal, and territorial government agencies; non-governmental organizations; Sector-Specific Agencies; and other Federal departments and agencies" and it generally reflects the current state of security standards for all organizations throughout the world. In some cases, other approaches and improvements have been proposed that show potential for more efficient protection or mitigation, and they are mentioned as well.

The Security Officer (SO)

Every organization, no matter how small, must designate someone to be responsible for both Physical and Cybersecurity, because once a Security Plan is in place, it must be continuously implemented, promoted, reviewed for effectiveness, and modified to incorporate responses to changes in the threat landscape.

In very small organizations, it may not be necessary to have a single person with the title of Security Officer. However, someone needs to be recognized as the person with the responsibility for instituting and operating the security program according to the Security Plan.

Ideally, the person will have a stake in the business beyond being an employee. Also, the chief security officer, although it may seem counter-intuitive, should not be a member of the IT staff. The vision of security perceived by the IT department does not protect the overall interests of the organization, and there are a number of conflicts of interest inherent between the operation of computers and networks and maintenance of an effective security plan. If the organization has an IT department, someone within it must be designated to implement the Security Plan, but should not have a major influence in instituting or changing the Security Plan.

These passages from the CISSP exam guide, clarify this issue:

"It is management's responsibility to set the tone for what role security will play in the organization. Management must decide what information is valuable and needs to be protected, who is responsible for protecting the data, to what extent employees may access and use the data, and what the consequences are for noncompliance."

"Many organizations incorrectly assume that Cybersecurity is a technical issue. It is not. Cybersecurity is a management issue that may require technical solutions." (Harris, 2010)

"When a company is hacked and thousands of customers' credit cards are stolen, intellectual property is taken, confidential information is leaked, or the organization's reputation is damaged, the management will be held accountable and expected to explain why due diligence and due care were not practiced in protecting the company and its resources. These explanations may be given to corporate offices, shareholders, judges, and customers. So it should be management who truly understand how security works within the organization and who should be calling the shots from the beginning." (Harris, 2010)

That being said, the managers of small organizations may not be qualified to completely assess the security requirements of the organization because they are not aware of all of the possible threats and they may not even be aware of the information their organization is storing or its value outside of the organization.

In these cases, outside help should be sought in the form of requests from supervising government bodies, paid consultants, or requests for pro bono help from security firms, educational institutions, etc. Of course, there is also a large amount of information available on the Internet, particularly from Homeland Security and other government sites that provide the complete set of risks from which the applicable ones may be selected. In every case the final plan should be reviewed by an experienced security expert, preferably from outside of the organization, and if possible, with experience with the specific type of business.

If a dedicated Security Officer is required, it goes without saying that the ideal individual should have an educational background in security coupled with relevant experience, preferably in the same industry as the hiring entity. Cybersecurity training and experience is far more important than computer programming or network experience. In fact, computer experience may be detrimental as it may result in a biased outlook on the overall approach to security.

Contrary to popular belief, programming skills are not required, or even necessary for a Security Officer. What is required is a deep and thorough understanding of what is involved in keeping an organization secure, and an employment environment that makes it possible to succeed. The SO must be able to show a propensity for constant learning and agility because the threat landscape is constantly changing and adjustments must be made quickly and effectively. A Security Certification is a good

indicator that a security professional has a solid foundation of knowledge/expertise and keeps it fresh through constant education.

Security can be a thankless job, because the measure of success is often that nothing happens. The Security Officer must have the marketing skill to constantly show that a great deal of planning, effort, and diligence goes into making sure that nothing happens.

This gives added importance to the SO's presentation of the detection and education components of the Security Plan. Every failed or thwarted attempt at exploitation should be reported for the dual purpose of showing diligent protection and the success of the Security Plan. If no attempts are made on the SO's own organization, reporting attacks on similar entities can be equally effective.

The selling or marketing of security is a major component of the SO's job because it serves to continually remind everyone that security is vital as is their role in it, and that security personnel are constantly working to protect the organization, its customers, and its employees.

The SO must be constantly visible, asking employees about security, encouraging comments and suggestions, along with reinforcing the importance of being vigilant. The SO should focus on meaningful approaches to educate employees about security to demonstrate the seriousness of the subject matter for the entire organization.

Ideally, the Security Officer should provide weekly or even daily messages reporting security activities and providing fresh tips on how each employee can help keep the organization and themselves safe. There should also be a Security Portal to provide all of the information employees will need to report any kind of incident and to serve as a point of contact for continuing education.

The Security Officer is the driving force in crafting a Security Plan, which, like so many things, is simple in concept, yet difficult in execution. There are five components, enumerated here and extended below: Identify, Protect, Detect, Respond, and Recover. Once the planning of the five components is complete, the challenge lies in the effective operation of the Security Plan.

The Security Challenge for Organizations with Small IT Departments

Security is a management responsibility. However, since such a large part of security now involves computer technology, it is very common to find that the organization's Security Officer is an employee in the IT department (for the purpose of this document all computer services departments will be referred to as the "IT department, regardless of what name they may use internally).

As previously noted, this is widely considered a poor decision for a number of reasons, including that an employee in that position will not have the credibility necessary to influence management and other departments, and the previously noted observation that anyone in the IT department does not have the proper broad perspective to safeguard the whole organization.

In an article in Forbes Magazine, written in the wake of the Target Stores data breach in 2013 entitled "Six Lessons from the Target Security Debacle", this is the final lesson:

"Sixth, and lastly, it is important to ensure that security be a board-level topic. Some companies are making the CSO[5] or CISO a peer to the CIO, and having that person report to the CEO. This is often a good idea, as it gives that executive a degree of objectivity and independence internally, and it ensures that that person will have the credibility and weight of opinion in board meetings. Companies should increasingly invite technology experts onto the board, as well, to ensure that all discussions are filtered through a security lens." (High, 2014)

If the security officer role currently exists, as part of one or more employee's job descriptions, management should consider elevating the position to management and outside of the IT department if it isn't already. Major corporations have been following this trend for years, as evidenced by these figures from the 2011 Global State of Information Security® Survey as reported in Wikipedia "About one-third of these security chiefs report to a Chief Information Officer (CIO), 35% to Chief Executive Officer (CEO), and 28% to the board of directors."

However, in the 2014 version of the above survey, only 17% of all respondents complied with these four requirements designated as indications of true leaders in security:

- Have an overall information security strategy
- Employ a CISO or equivalent who reports to the CEO, CFO, COO, CRO, or legal counsel
- Have measured and reviewed the effectiveness of security within the past year
- Understand exactly what type of security events have occurred in the past year (Cooper, 2014)

The most important point is that the person managing the Security Plan should not be a member of the IT department. However, there must be persons in the IT department to run the security processes required to implement the plan under the direction of the SO.

If the enterprise does not have an IT department at all, and does not choose to hire an employee for this purpose, an outside firm may be retained to provide the basic security technologies that require constant monitoring and updating, such as firewalls, spam filters, inbound and outbound network traffic monitors, threat scans, blacklists,

[5] CSO is Chief Security Officer, CISO is Chief Information Security Officer.

whitelists, etc. If the Security Plan specifies threats not covered by contract security, the SO must find and implement solutions.

If the organization is in a Critical Infrastructure industry, the risk of not having an independent SO are so large as to be unbearable, particularly with the partnerships and grants available through all levels of government designed to aid CI organizations in building effective security in accordance with the Presidents directives, the most recent of which, number PPD21, was issued in February of 2013, stating "It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure, considering all hazards that could have a debilitating impact on national security, economic stability, public health and safety, or any combination thereof. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure." (States, 2013)

The Security Plan

For the sake of basic survival, every organization needs a Security Plan. There are many cybersecurity philosophies defined by groups such as the major professional certification bodies: CompTIA (Computer Technology Industry Association), SANS (originally SysAdmin, Audit, and Network Security) and (ISC)²® (International Information Systems Security Certification Consortium), but all of them agree on several major points:

Any effective cybersecurity model uses a multiple level, redundant approach. CompTIA refers to it as "Security in Layers", SANS describes it as "Defense-In-Depth" (DID), and the (ISC)2 guide refers to it as "A Layered Approach". The SANS Institute specifies four different approaches: Uniform Protection, Protected Enclaves, Information Centric, and Vector Oriented.

The (ISC)² model is based on the 10 Domains in the Common Body of Knowledge (CBK®):

1. Access Control
2. Telecommunications and Network Security
3. Information Security and Risk Management
4. Application Security
5. Cryptography
6. Security Architecture and Design
7. Operations Security
8. Business Continuity Planning and Disaster Recovery

9. Legal Regulations, Compliance, and Investigation
10. Physical (Environmental) Security (Harris, 2010)

Regardless of which approach is used, the principle is the same: "…a good security architecture, one that can withstand an attack, has many aspects and dimensions." and "…if one countermeasure fails, there are more behind it." Finally, if all else fails, it should "…be ready to detect that something has happened, clean up the mess completely and expeditiously, then tune … defenses to keep it from happening … again." (Institute, 2014)

As noted above, the Security Plan, or Framework Core in the cybersecurity Framework, consists of five functions: Identify, Protect, Detect, Respond, and Recover which should include all of the previously mentioned aspects of security.

Identify - What Must Be Protected (Risks)

The first step is to identify what must be protected (risks) and how it can be compromised (threats) and to prioritize the risks and threats (vulnerabilities). Use the "CIA" triad principals to define risks (sometimes called the AIC triad): Confidentiality, Integrity, and Availability (Institute, 2014) (Harris, 2010). If any of these principles are violated, the security of the system may be compromised:

Confidentiality – Much, if not most of the information in an organization's computer system could cause damage if it were made available to outside parties, either because it is sensitive information subject to misuse, or because it would provide information about inner workings that could be damaging, misinterpreted or used by outsiders to cause negative outcomes.

Integrity – If the information becomes inaccurate or unreliable, any activity based on it may be severely impaired if not rendered completely worthless.

Availability – If the information is not available when it is needed, there may be serious consequences.

The order of importance of the CIA principles will vary by industry. An example of this in the SANS guide is an online school that needs the enrollment process to be available to stay in business, and so gives it the highest priority. However, while the order of the CIA principles may be used in planning and may govern the allocation of resources, it must be emphasized that these are "bedrock" principles and each one must be completely addressed before allocating additional resources. (Institute, 2014)

Another way to look at the same principles from a different point of view is the AAA Architecture :

Authentication – confirm identity

Authorization – permission for activities and resources

Accounting – track all resource usage and attempts

While most if not all security texts refer to the items to be protected as “assets”, this can be dangerously misleading. The term “asset” universally denotes that the item in question has a monetary value. In the arena of cybersecurity, the items protected often have no financial value whatsoever.

For example, employee information including address and Social Security Number has no value to an employer, but great value to identity thieves. Other items may be very valuable to outside interests, yet their value may be very obscure to those without security experience. Good examples of this type of information are routable internal network addresses and employee permissions.

If a hacker obtains routable internal addresses, they will have a door into the network and could use it to gain entry to anything connected. If saboteurs know which employees have access to the programs or equipment they want, it makes their jobs much easier. Again, these items are not “assets” by any conventional definition, but they represent a critical risk and must be protected.

Making a complete list of everything that is to be protected is imperative. This list must always be as comprehensive and current as possible. Developing the list, along with the attendant Security Plan document is a collaborative activity that must involve management from all areas of the enterprise, along with operational and technical representatives. Writing and publishing the Security Plan should be viewed by the organization as an essential project vital to the on-going health of the entity.

The list should be reviewed by security experts, hired from outside if necessary. If this is not done, items will inevitably be overlooked. Information that may be appraised as having little or no value internally, or that no one is even aware of can be of great import to outside entities.

While physical plant security is an important component of the Security Plan, it will not be covered here. An excellent example of a plan incorporating physical security is, in my opinion, the Federal Energy Regulation Commission (FERC) security plan example for hydropower facilities at this link (FERC, 2014): http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security-plan-example.pdf .

This plan includes specifications for such physical protections as Fencing and Gates, Exterior Lighting, Closed-circuit Television (CCTV), Electronic Access Control, Intrusion Alarms, Security Guards, etc., the complete set of which would be too much for most organizations where a subset would be sufficient.

The first step in identifying non-physical plant risks is for upper management to prepare a list of protection priorities based on what information is necessary to keep the enterprise running. Secondly, identify any information that could compromise the

integrity or reputation of the enterprise should there be a data breach, as illustrated by the Ponemon/IBM and Verizon studies mentioned previously and below.

The IBM-Ponemon 2014 Cost of Data Breach Study for the United States revealed these points (Institute, 2014):

- The average cost of a data breach increased from $5.4 to $5.9 million, and the cost per record increased from $188 to $201.
- 15% more customers ended their relationship with companies experiencing data breaches (comparing 2013 and 2014 surveys)
- "Malicious or criminal attacks rather than negligence or system glitches were the main causes of data breach."

"If the organization has a strong security posture or a formal incident response plan in place prior to the incident, the average cost of a data breach was reduced as much as $21 and $17 per record, respectively."

Even with the expensive risk caused by the loss of data, the GSISS-2014 showed a disturbingly low percentage of respondents using several critical areas of asset protection, coupled with a decline in use from 2011 to 2013:

- Classifying business value of data (down from 22% to 17%)
- Procedures dedicated to protecting IP addresses (down from 22% to 20%)
- Inventory of assets/asset management (down from 29% to 26%)
- Regular review of users and access (down from 37% to 31%)

This information emphasizes the fact that it is important to identify risks and establish strong protection strategies, not only to prevent exploits, but because it serves to preserve the integrity and reputation of the exploited enterprise, and may even lower costs in the wake of a security breach. In other words, a solid Security Plan works, even if it fails.

The aforementioned Verizon survey finds that 92% of all security breaches fall into nine broad areas, making it an excellent starting place for building a Security Plan:

1. Point of Sale Intrusions – While this vulnerability seems to apply mostly to retail businesses, it affects any organization that accepts credit cards for payment or uses systems similar to Point of Sale (POS) terminals. This problem is also largely concentrated among small to medium-sized businesses, in spite of all of the news concerning large retailers. These attacks may subject customers to all of the misfortunes of identity theft, which will in turn be reflected back against the organization.
2. Web App Attacks – These types of attacks are generally aimed either at using the web app to gain entry to data on the server or network, or hijacking the site to post a message or use in a Distributed Denial of Service (DDos) attack

on another site. Most vulnerable are sites using off-the-shelf or shareware content management systems like Drupal, WorkPress, or "Joomla!", and are in the Information, Utilities, Manufacturing, or Retail industries. Attacks can cause performance problems, reputation damage, lost data, etc.

3. Insider and Privilege Misuse – The Edward Snowden case in the news is an extreme example of an insider who misused his legitimate privileges in a way that caused a large amount of damage to his employer. This exploit affects any organization with valuable secrets that may be exposed by trusted employees or contractors.
4. Theft and Loss – While this category is governed mostly by physical security, computers and tablets are among the items most often lost or stolen, so there should be a cyber-component in all of the following steps.
5. Miscellaneous Errors – The most common errors in this category are sending sensitive data to the wrong recipients, posting secret data on a public site, improper disposal of media containing data. These errors can be every bit as damaging as criminal acts.
6. Payment card skimmers – This category is primarily physical as skimmers are devices that are attached to credit card scanners to record the information from the scanned card.
7. Denial of Service – Denial of Service (DoS) attacks can completely shut down organizations that depend on a web site for their livelihood. They are also one of the most difficult exploits to defend against, particularly when multiple faceted Distributed Denial of Service (DDoS) versions are used. Web sites are not the only targets. These attacks are becoming more sophisticated, using hijacked high-bandwidth servers to launch not only traditional UDP and SYN floods, but HTTPS GET requests.
8. Cyber Espionage – Verizon reported triple the number of espionage reports in 2013, with "a wider variety of threat actions than any other pattern." Not surprisingly, the most frequently attacked identified target for espionage was the public sector (federal, state, and local government agencies and related entities). However, firms in the Professional and Manufacturing sectors reported significant numbers as well, almost evenly distributed between small and large organizations.
9. Miscellaneous – Includes mostly external hacking of individual sites, and various phishing schemes.

Obviously, identification is at least 50% of the plan and if it isn't done meticulously and as comprehensively as possible, the security plan has little chance of success. If the organization falls into the trap of trusting the "packaged solution" mentality by buying a firewall or threat gateway and packaged software, and trusting outsiders to protect them, there will be the same low rate of success. Even if an organization has substantial resources, such as Target, for example, their success in protecting their

organization is still dependent on having an effective security plan and executing it properly.

Once the risks have been identified, quantifying them into vulnerabilities is equally as crucial, because this creates an order of importance so the most effort and resources are concentrated on the areas that are most likely to hurt the organization.

This is where generic solutions fail because they try to protect against every possible threat, including many that are not important or applicable to the individual entity. As the Verizon DBIR demonstrates, most organizations are particularly susceptible to one or two types of threats, representative of the type of industry to which they belong.

It is important to get the big picture by extrapolating the effects of security breaches, and looking at history when evaluating the severity of the risk. Often the cost of the event is not direct – Target did not lose any money when charge records were stolen, and their business was not disrupted while the breach was happening. It was only afterward, when the incident was publicized and customers became aware of the risk they had been unknowingly subjected to that the cost began to be realized.

Of course, in today's world, most retailers understand the consequences of leaking customer information and consider its protection to be among their highest priorities, but other industries have equally large risks that may not be so universally understood. It is vital for managers in every industry to project the potential consequences of any security breach and adjust the risks accordingly.

Part of the identification process should include an analysis of future plans for at least five years. Changes of location, migrations of software and technology, equipment addition or replacement, expansion, staff changes, etc. are risks and should be included in the Security Plan.

It is important to be aware of cybersecurity events that are occurring in the outside world and evaluating their threat potential to one's own organization. Web sites such as The Open Web Application Security Project (OWASP), OUCH! The SANS security awareness newsletter, and Bruce Schneier's Crypto-Gram newsletter are excellent sources for this research. (OWASP, 2014)

All compliance activities, such as with government regulations (PPI, HIPA, Sarbanes-Oxley, industry-specific), external or internal policies, etc., must be recognized as a risk in themselves and as a controlling factor in measuring related risks. For example, the failure to meet a documentation retention policy represents, because of fines, a financial risk, while meeting it may increase the security risk by raising the amount and sensitivity of information to be protected.

Often overlooked in security planning is that the very implementation of the effective security plan may create or exacerbate existing threats. The most common and significant area of concern is the effect that the security plan may have on employees.

If the plan appears to negatively impact personnel, or if the operators of the plan abuse it, employee morale may turn negative.

Of all of the threats to the security of an organization, the most dangerous and underestimated is that of disenfranchised and hostile employees. The effectiveness of the Security Plan is totally dependent upon the complete collaboration of all employees, through mutual trust and respect.

Protect – Stop it from happening in the first place

Once the risks, threats, and vulnerabilities have been determined, protection protocols must be devised, using internal history along with guidelines provided by historical tools such as the Verizon and Ponemon/IBM reports, the NIST Cybersecurity Framework, GSISS-2014, security firm guidance, etc.

There is plenty of room here for innovative solutions, because the commercially available tools are generic and may be highly configurable. There are also a number of ways to create tailored protection based on data and policies that are unique to each individual enterprise and are unknown to those who would exploit them.

GSISS-2014 specifies the following security technologies with the percent of respondents implementing them:

- Policy-based network connections to detect and/or counter security incidents (68%)
- Inspect inbound and outbound network traffic (61%)
- Account/password management to reduce security incidents (60%)
- Acceptable-use policy (55%)
- Malware analysis tool to counter advanced persistent threats (APTs) (51%)
- Data loss prevention technology (51%)
- Security event management (50%)
- Cyber-threat research (25%)
- Not allowing non-corporate-supplied devices in the workplace/network access (17%)

The Cybersecurity Framework lists the following generalized methods of protection:

1. Access Control
2. Awareness and Training
3. Data Security
4. Information Protection Processes and Procedures
5. Maintenance
6. Protective Technology

The Verizon Data Breach Investigations Report gives more specific advice for each breach type. For example, to prevent Cyber Espionage, they suggest:

A. Keep software up-to-date with the latest patches to minimize vulnerability to exploitation based on bugs.
B. Use and update an Anti-virus program.
C. Train users to give them the knowledge and skills to recognize problems and respond accordingly. Over the years this has been shown to be the most effective component for discovering espionage.
D. Segment the network to contain incidents.
E. Make sure important activities are logged and the logs are monitored. This may help in repairing the problem and preventing a recurrence.
F. Maintain constant vigilance against phishing attacks. History shows that it only takes 10 attempts to be successful, so using every possible method to prevent the phishing message from getting through is warranted, including spam detection, block lists, email header analysis, pattern matching, and sandbox analysis of attachments and links, and use Data Execution Prevention (DEP)and Endpoint Threat Detection and Response (ETDR) solutions.
G. Get threat indicator feeds and watch both incoming and outgoing data for deviations from the norm.
H. Lateral movement inside the network is enabled by user accounts with too much authority, and can be slowed or stopped by establishing an effective authority hierarchy, using two-factor authentication and watching for unusual user login activity.

No protection scheme is going to work completely or forever. This is where a diligent Security Officer is important because the protections have to be constantly monitored and adjusted based on internal information and changes in the overall threat landscape.

Detect – timely discovery of cybersecurity events

Above, in the 8 steps (A through H) to protect against Cyber Espionage, several of the methods actually overlap with the detection step in the security plan. In practical usage these two steps are inseparable, yet distinct. The only way to determine if protection is working is through detection.

The Cybersecurity Framework gives the following 3 examples of "outcome categories" to enable "…timely discovery of cybersecurity events" (Technology, 2014):

1. Anomalies and Events
2. Continuous Monitoring
3. Detection Process

All three of these categories describe essentially the same thing because the purpose of monitoring is to detect anomalies and events that indicate a security event or attempt. The Verizon DBIR document has some more detailed examples under the same general heading of detection:

Step E above mentions computer logs. These are text documents that are created by running processes on various computers and other devices in an organization's network. Usually, these logs have to be turned on and configured by administrators to begin journaling the requested information. The security plan must specify what information should be captured in the log files and for how long they should be kept.

If configured correctly, the log files may be the best source of information about the current state of the entire internal computer universe, as well as a historical document to aid in determining if anything has happened that bears examination. Most networks will have too many logs to monitor manually and will require some form of Log Management, which will also include tools to automatically produce alerts for suspicious activities or events.

The Verizon DBIR's step F, "maintain constant vigilance against phishing attacks", is a good example of continuous monitoring. Effective monitoring requires multiple sets of eyes. The output from email monitoring and anti-virus software must be monitored constantly, and there must be live monitoring as well.

Services such as FireEye, mentioned below, can be hired to oversee all communications and report suspicious digital patterns. It is also important to acquire monitoring packages that provide easy to read dashboards so the network can be monitored by personnel without extensive training, and can produce automatic alerts in case of critical system failures or programmed anomalies.

Respond – What to do when something happens

As Bruce Schneier, one of the world's foremost security experts says, "Prevention is ideal but detection is a must; however, detection without response has minimal value."

"All of those next-generation endpoint detection systems, threat intelligence feeds, and so on only matter if there is action taken, a reaction to the information. If Target had had incident response procedures and a system in place to ensure they followed those procedures, it is more likely there would have been a response to the alerts received from FireEye[6]."

"This is why I believe that incident response is the most underserved area of IT security right now." (Schneier, 2014)

This previous statement by Mr. Schneier was in response to the article below detailing how a Target had a chance to avoid a major breach:

"In testimony before Congress, Target has said that it was only after the U.S. Department of Justice notified the retailer about the breach in mid-December that

[6] FireEye™ is a computer security firm that provides security detection and prevention software, including the $1.6 million malware detection tool used by Target. Their web site is located at http://www.fireeye.com.

company investigators went back to figure out what happened. What it hasn't publicly revealed: Poring over computer logs, Target found FireEye's alerts from Nov. 30 and more from Dec. 2, when hackers installed yet another version of the malware.

Not only should those alarms have been impossible to miss, they went off early enough that the hackers hadn't begun transmitting the stolen card data out of Target's network. Had the company's security team responded immediately, the theft that has since engulfed Target, touched as many as one in three American consumers, and led to an international manhunt for the hackers never would have happened at all." (Riley, et al., 2014)

Recover – What to do to resume normal operations

The NIST Cybersecurity Framework defines this element as "Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications." (Technology, 2014)

Recover, in the context of the Security Plan is not generally the same as the organization's Disaster Recovery Plan, although it could be, as in the case of the attack on PG&E's Metcalf power transmission substation, which knocked the facility completely out of service for 27 days. (Smith, 2014) At that point, with the plant shut down, they had no choice but to go to their disaster recovery plan, which was to have other facilities absorb the slack until they could get back on line.

Normally, recovery from a security event falls short of evoking the Disaster Plan, unless it incorporates a detailed Enterprise Continuity Plan that anticipates and plans for any possible event that requires recovery. One thing for certain; if a Security Plan with a recovery section is not in place, the effects are more likely to result in a complete shutdown or reversion to the worst case scenario.

The recovery phase of the Security Plan should be viewed as a continuity plan. It must specify, for each risk, what will be done to either quickly repair or work-around the consequences of the security breach. It should also set a threshold for progression to more serious actions, such as a temporary shutdown or full disaster recovery.

In the case of Critical Infrastructure (CI) organizations, there must also be coordination with government agencies as well as other organizations in the industry, as in the case of the disabled power station, where other organizations had to increase capacity or take other steps to continue services while the affected unit recovered. (Kirk, 2014)

Implementing the Security Plan

Putting a security plan into motion is similar to an advertising or motivational campaign except that the stakes are much higher, since everyone's job, and the continuing existence of the organization, and whatever service it provides to the public are potentially at risk. Every employee needs to be aware of the Security Plan and dedicated to its implementation.

Without a dedicated Security Officer, this implementation becomes difficult and is less likely to be effective. Half-hearted attempts to implement security may communicate a lack of commitment which the employees will notice. They need to take the security plan seriously. Less than stellar examples include Security Policy and acceptable-use documents posted on an internal web site, annual quizzes accompanied by slide shows and YouTube-type security videos, and establishing as the "Security Officer" someone who has a full-time job doing something else that takes precedence over all security activities.

"Alignment" is the key word for an effective Security Plan implementation. In order to secure participation from management, the Security Plan must be aligned with the goals of the business. The same goes for getting employees involved, although their participation may require some augmentation.

A management team cognizant of the most recent news stories and estimates of the costs of security breaches should require little to be convinced that an effective Security Plan is in each of their best interests as well as that of the organization. As previously asserted, security is a management responsibility, so avoiding the consequences of ineffective security should be high on the lists of goals.

So management along with employee backing is crucial for successful implementation of a Security Plan. As all of the surveys quoted above have shown, the greatest threat to any operation comes from within. These are ways to attack the threat by encouraging employee participation:

1. Periodic security meetings to introduce employees to the Security Plan and emphasize how the benefits of effective security apply to them. This could be piggy-backed onto other periodic meetings such as department and enterprise-wide meetings. Any time a significant number of employees are brought together, the SO should be there with a fresh security promotion.
2. The Security Plan, along with posters and newsletters should be posted throughout the physical plant, and frequent broadcast emails should be sent and postings should be frequently made on the company web site. There are numerous sources for cybersecurity posters and promotional material available by doing a web search for "cybersecurity posters and banners".
3. Phishing is the most dangerous computer exploit and can be eliminated entirely by educating management and employees to recognize it and report

incidents so they can be blocked. There should be a meeting at least once per year on phishing, with actual examples from the organization.

4. There should be meetings every year with each employee to go over the acceptable-use policy, making sure that everyone understands it and agrees to it by signing. Other security topics should also be covered.
5. Security training should be part of the required curriculum for every employee and should be included in the formal training program.
6. Institute a prize system, even if there is no money for prizes. Ask managers for donations of gift cards, sporting event, museum, concert or movie tickets, and try to arrange traditional non-monetary incentives such as days or hours off, lunch with a higher-up, close-in parking, etc. Give prizes for discovering and immediately reporting phishing emails, or people trying to enter the office without badges, or passwords written on post-it notes by an employee's desk, etc.
7. Use crowd-sourcing to help with security by opening up the CCTV systems and alert dashboards to employees to monitor on the network. Anyone spotting something and reporting it gets a shout-out and a prize. Employees should also be encouraged to visit other areas of the enterprise and look for security problems.
8. Employees should know that security is an integral part of their job and it should be included on the standard periodic evaluation, not as a rating item, but as a reminder of the importance of security.

The effectiveness of the Security Plan should be evaluated continuously and formally reported at least once a year, using criteria built into the plan itself.

All changes to the Security Plan should be made at once and distributed to all locations where the plan is available (which should be everywhere) as well as online. Changes should result from the on-going evaluation of the plan, as well as from constant analysis of security reports from the outside world, as they may affect the organization.

Conclusion

Because of all of the threats arising from the use of computers and the Internet, every organization needs a Security Plan and a Security Officer. Even a one-person company needs an organized plan to avoid exploits such as phishing and identity theft.

A Security Officer is a necessary first step toward building an effective Security Plan. If a dedicated SO is not warranted or possible, a manager or team of managers should take the responsibility. The SO should not be an employee in the IT department.

The SO and management should build the Security Plan using a template such as the FERC Sample below, using the following guidelines:

- Identify - decide what needs to be protected, then assess a risk value so it can be prioritized
- Protect – determine protection strategies and products for each risk item
- Detect – design methods for finding out when protection has been defeated and reporting the violation to the Security Officer and designated responders
- Respond – determine what to do when a breach is detected and assign responders.
- Recover – for each protected type as well as any unforeseen action, design a recovery strategy, up to and including the Disaster/Recovery worst case scenario of total destruction and shutdown

Once the Security Plan is complete and approved by management, every employee in the organization needs to be informed that its implementation is an essential aspect of their job. The Plan should be posted, both online and a hard copy easily accessible and an audio version available, if necessary, so it can be referred to at any time by anyone.

Because of the ever-changing threat, the Security Plan will remain fluid, rather than fixed policy to be filed away. Management and the Security Officer must be committed to devoting the time and resources necessary to ensuring the Security Plan is an on-going priority. Updates/evaluations will be necessary whenever almost anything system related changes. Sometimes a change will be necessary, revealed through experience, research or outside advice. Success is contingent upon the commitment of management and staff.

FERC Sample Security Plan

http://www.ferc.gov/industries/hydropower/safety/guidelines/security/security-plan-example.pdf

Works Cited

Blair, Nancy. 2014. AOL says it's investigating security breach. *USA Today.* [Online] April 28, 2014. [Cited: May 25, 2014.] http://www.usatoday.com/story/tech/2014/04/28/aol-spoofed-emails-security-breach/8429601/.

Bradley, Tony. 2014. the-top-5-security-threats-to-watch-for-in-2014.html. *PCWorld.* [Online] January 30, 2014. [Cited: May 16, 2014.] http://www.pcworld.com/article/2092226/the-top-5-security-threats-to-watch-for-in-2014.html.

2014. Category: Vulnerability. *OWASP.* [Online] owasp.org, April 5, 2014. [Cited: May 25, 2014.]

Commission, Federal Trade. 2009. Health Breach Notification Rule 16 CFR Part 318 [RIN 3084-AB17]. *Federal Register.* s.l. : Federal Register, 2009. Vol. 74, 163.

Cooper, Price Waterhouse. 2014. The Global State of Information Security Survey 2014. *pwc.* [Online] 2014. [Cited: May 25, 2014.]

Essers, Loek. 2014. Hackers access user personal data stored by eBay. *Computerworld.com.* [Online] May 21, 2014. [Cited: May 23, 2014.] http://www.computerworld.com/s/article/9248484/Hackers_access_user_personal_data_stored_by_eBay?source=CTWNLE_nlt_security_2014-05-22.

FERC. 2014. Federal Energy Regulatory Commission. *FERC.gov.* [Online] April 25, 2014. [Cited: May 17, 2014.]

Harris, Shon. 2010. *All-In-One CISSP Exam Guide.* s.l. : The McGraw-Hill Companies, 2010.

High, Peter. 2014. Six Lessons From The Target Security Debacle. *Forbes.* [Online] May 5, 2014. [Cited: May 25, 2014.] http://www.forbes.com/sites/peterhigh/2014/05/05/six-lessons-from-the-target-security-debacle/.

ICS-CERT. 2014. Year_In_Review_FY2013_Final.pdf. *ICS-CERT.* [Online] May 15, 2014. [Cited: May 15, 2014.] http://ics-cert.us-cert.gov/sites/default/files/documents/Year_In_Review_FY2013_Final.pdf.

Institute, Ponemon. 2014. *2014 Cost of Data Breach Study: United States.* s.l. : IBM and Ponemon Institute, 2014.

Institute, The SANS. 2014. *Security 401 - Security Essentials Bootcamp Style 401.2 Defense In-Depth.* s.l. : The SANS Institute, 2014.

Kirk, Jeremy. 2014. Public utility compromised after brute force attack, DHS says. *ComputerWorld.com.* [Online] May 21, 2014. [Cited: May 23, 2014.] http://www.computerworld.com/s/article/9248473/Public_utility_compromised_after_brute_force_attack_DHS_says?source=CTWNLE_nlt_security_2014-05-22.

2013. NIPP 2013 – Partnering for Critical Infrastructure Security and Resilience. *Department of Homeland Security.* [Online] 2013. http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience.

Riley, Michael, et al. 2014. Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. *Business Week/BloombergBusinessweek Technology.* [Online] March 13, 2014. [Cited: May 24, 2014.] http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

Schneier, Bruce. 2014. Crypto-Gram Monthly Newsletter. *Schneier on Security.* [Online] 4 15, 2014. [Cited: 4 18, 2014.] https://www.schneier.com/crypto-gram-1404.html.

Security, United States Department of Homeland. 2014. What is Critical Infrastructure? *Official Website of the Department of Homeland Security.* [Online] May 11, 2014.

Smith, Rebecca. 2014. Assault on California Power Station Raises Alarm on Potential for Terrorism. *The Wall Street Journal.* [Online] February 5, 2014. [Cited: May 17, 2014.] http://www.marketwatch.com/story/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-2014-02-04-224493020.

States, President of the United. 2013. Presidential Policy Document 21. *The White House.* [Online] 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Steve Frank, APR. 2009. *Metro Wastewater Reclamation District, A 45-Year History.* Denver, Colorado : Metro Wastewater Reclamation District, 2009.

Technology, NIST - National Institute of Standards and. 2014. *Framework for Improving Critical Infrastructure Cybersecurity.* NIST. s.l. : NIST, 2014.

Wide-Area Situational Awareness for Critical Infrastructure Protection. **Alcaraz, Cristina and Lopez, Javier, University of Malaga, Spain. 2013.** 4, s.l. : Computer.org, April 2013, Computer - IEEE Computer Society, Vol. 46, pp. 30 - 37.