ASIS UTILITIES SECURITY COUNCIL

UTILITY SECURITY RISK MANAGEMENT

SECURITY PROGRAM FUNDAMENTALS

ASIS INTERNATIONAL®
Utilities Security Council

[This page is intentionally left blank]

ASIS UTILITIES SECURITY COUNCIL

UTILITY SECURITY RISK MANAGEMENT

SECURITY PROGRAM FUNDAMENTALS

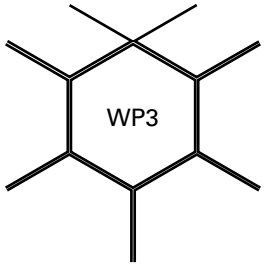


Table of Contents

Acknowledgments

ASIS members are unpaid, expert volunteers, contributing their time and expertise to continuing education of fellow security practitioners. In addition to the efforts and sponsorship from ASIS Councils, the following individuals assisted in the research and compilation of this project. Their work is greatly appreciated.

Contributors

Doug Powell, CPP, PSP
British Columbia Hydro & Power Authority

Scott Starkey, CPP, PSP
Birmingham Water Works

Allan Wick, CPP, PSP, PCI, CFE
Tri-State Generation & Transmission

Paul Stanley, CPP
British Columbia Hydro & Power Authority

Chris McColm, CPP
Manitoba Hydro

Peer Reviewers

Doug Powell, CPP, PSP
British Columbia Hydro & Power Authority

Scott Starkey, CPP, PSP
Birmingham Water Works

Scott Stephens, CPP
Austin Water Utility

Allan Wick, CPP, PSP, CPI, CFE
Tri-State Generation & Transmission

Chris McColm, CPP
Manitoba Hydro

Paul Stanley, CPP
British Columbia Hydro & Power Authority

ASIS INTERNATIONAL
Advancing Security Worldwide®

Introduction

The foundation of security management in any industry is sound risk management. Yet in many instances of security management, far too common the essential risk management program is inadequate or lacking. There has been growth in the adoption of threat-risk assessment even though vulnerability assessments and threat assessments are often packaged and sold off as risk assessment. To clarify, threat and vulnerability comprise important and necessary components of a risk assessment, but neither should be confused with risk assessment when taken in isolation.

Various forms of threat-risk assessments exist today, applied in different industries to varying degrees of accuracy and effectiveness. Paper-and-pen assessments rely to a large extent on the personal knowledge and experience of the assessor, and these types of assessments and others of the past provide little more than a cursory overview of a limited number of security risks, based on a sampling of a few threats, and often based on an already existing security problem or concern. Consequently, meaningful threats or vulnerabilities may not have been identified and mitigation was misaligned or misses the security issue entirely, causing undue scrutiny on the cost-benefit and return on investment of the security department. Consider, what would happen when a mitigation recommendation is returned that $100,000 in new fencing is needed to resolve a theft problem at a facility rife with workplace violence and public safety incidents? One would expect raised eyebrows from company executives and finance managers. It may have been imperative that the facility receive a fencing upgrade, but the assessment was neither complete nor correct for the business needs, nor solves the priority security issues. Fences do not, by themselves, provide effective protection.

Current Utility Assessment Frameworks

Many of the advancements in comprehensive risk management are made in critical and high-risk environments (e.g., nuclear generation, gas and oil, and dam safety). The rise in global terrorism further escalated risk assessment activity. For familiarization purposes, what follows are summaries of a few established assessment frameworks applied by utilities.

The Federal Energy Regulatory Commission (FERC) in the United States provides a dam safety risk and vulnerability assessment tool based on a disaster management model wherein vulnerability pertains to the potential for catastrophic impacts on society through dam failure or destruction of individual assets related to dam operations. The Dam Assessment Matrix for Security and Vulnerability Risk (DAMSVR) assessment has made slight shifts in methodology to consider, for example, impacts on populated areas as opposed to fatality estimates if dam failure is realized. This assessment culminates in tables where dam rankings are generated as a result of the assessment work. These rankings relate to risk levels and should lead a dam owner to apply security planning and barriers commensurate with the risk importance of that dam. Other assessments in this group exist for transmission systems, distribution systems, and so forth. In this example, risk is related to impact on society, not merely impact to the utility and/or critical infrastructure (e.g., loss of power generation).

The U.S. Nuclear Regulatory Commission (NRC) provides a probabilistic risk assessment (PRA) guideline that looks at probability in terms of frequency of various incident types, then uses fault tree analysis and modeling to achieve escalated levels of containment. Divided into three PRA levels, an incident will pass through plant

response, core and containment response, and external influences modeling to determine consequential values. In terms of barrier applications, the more suitable a set of mitigations at each level, the lower the consequential values resulting from a serious incident. PRA is explained in the following way on NRC's official website, "The NRC uses Probabilistic Risk Assessment (PRA) to estimate risk by computing real numbers to determine what can go wrong, how likely is it, and what are its consequences." Thus, PRA provides insights into the strengths and weaknesses of the design and operation of a nuclear power plant. For nuclear power plants operating in the United States, a PRA estimates three risk levels:

- A Level 1 PRA estimates the frequency of accidents that cause damage to the nuclear reactor core. This is commonly called core damage frequency (CDF).
- A Level 2 PRA, which starts with the Level 1 core damage accidents, estimates the frequency of accidents that release radioactivity from the nuclear power plant.
- A Level 3 PRA, which starts with the Level 2 radioactivity release accidents, estimates the consequences in terms of injury to the public and damage to the environment.

While the approach is different to risk assessment, these two industries view vulnerability as the ability of the utility entity to control various impacts in terms of how these impacts affect the human population. By comparison, other risk assessments will view vulnerability according to impacts on the business itself. This does not mean that the nuclear industry or the dams sector does not consider the impacts on their business operations. They do. In fact, the loss of power generation or water supply is directly related to the socioeconomic well-being of society relative to the size and value of the asset to society (as a power generator, water supplier, flood control, etc.). Ultimately, barriers and controls should match the asset ranking and ultimate vulnerability assessed. Where many industries have lost their focus in past decades is not in coming to some agreement on the risk associated with assets like these but rather on the ongoing need to maintain these barriers and refresh risk assessment based on a changing environment. For example, in the water industry's guidelines, the risk assessment should be updated at least every three to five years. The changing environment will continually shift norms and add changing threat values to the assessment. Threat-risk assessment, as the name implies, should be a comprehensive and ongoing evaluation of these values.

Among the prominent and well-developed commercial physical security risk assessment packages available today is one that began as a tool for combating gang activity in Los Angeles. Asvaco™ Assessment Services (www.asvaco.net) was founded by first responders in 1998, and its development over the years has led it to become the leading software in the area of risk assessment. What makes their software relevant in the field of security risk assessment, in part, is not just its many years refinement but the product's move to a comprehensive methodology of asset ranking, threat ranking, vulnerability impact analysis, and consequence definition; allowing the user to refine assessment values and define impact according to company risk assessment values. It was also designed using effective standards for assessing impact. Tools like the Asvaco assessment consider security risk assessment from a threat overview and make use of historical crime data, company incident data, known threat agent values, geological, meteorological, and other data to complete analysis. All of this combines to make the threat analysis relevant to the company performing the assessment. The tool then uses a comprehensive set of standards (NFPA 1600; FEMA 452, initially) to ensure that the assessment and resulting recommendations are based on standards.

IT Risk Management

Commonly within IT risk management, strategic IT asset risk assessed against prevailing IT security standards like ISO/IEC 27000, which includes 27001–27006 and typically focuses on 27002 as a comprehensive security policy set.[1] Determining critical cyber assets (*see* NERC-CIP assessment) in a structure assessment of asset vulnerability weighted against the loss of the asset provides a hierarchical view of the IT infrastructure of the company and the relative priority of asset protection, including disaster recovery needs. The more critical an asset is, the less downtime that can be planned for. Prevailing threats are mitigated with standard security practices outlined in the corporate information management system, dictating protection standards by asset classification. Therefore, we would expect to see a higher level of information protection (encryption, certificates, etc.) and access control (passwords, biometrics, etc.), as well as a higher level of patch management, version control, security of the asset itself, and so on for a critical asset as opposed to a lower-level asset.

Within IT, security vulnerability assessment (VA) is often equated with risk management. Overall IT risk management use ongoing vulnerability scans, but a vulnerability assessment does not equate risk management. Risk management for IT systems should also consider threat agent capability, prevailing threats and threat trends, and also some deeper form of vulnerability assessment like penetration testing. In fact, disparate standards may have to be considered besides a single overarching security standard like ISO 27002 to fully measure compliance in the IT risk assessment. In fact, governance takes a prominent role in IT risk assessment (as it should in a physical assessment) given the nature of IT infrastructure, especially viewed in the historical context where various IT assets are distributed throughout a utility. IT assets and systems distributed amongst many business groups and over a large geographic footprint make use of multiple types of networks for data transmission and may not have been well designed or controlled over the years, meaning nonstandard, personal, and rogue IT systems may be in use throughout the company. Managing IT governance and compliance becomes a huge part of utilities security risk management.

The expansion of utilities assets into the public domain—especially as it relates to the proliferation of IT assets in the smart grid and control systems—increases attack vector potential, placing a larger number of assets at risk. The public domain is a complex environment to manage anything within. Placing millions of IT assets into the public domain would suggest that security risk management will also become extremely complex. Adding multiple commercial IT applications to the mix makes this extremely risk-sensitive. An attack vector is simply a way in and does not necessarily speak to vulnerability. The point here is examining vulnerability and associated risk is necessary to ensure appropriate risk management.

Utilities security risk management will progress with more astute and knowledgeable security professionals to undertake the task of managing this risk. Integrated security risk management becomes more important in this environment and will require critical thinking in terms of roles and responsibilities. Meeting an enterprise model for risk management, and educating the enterprise to security risk management needs and priorities are equally important. Finding and using the right tools with the right degree of expertise is essential in framing

[1] *Information technology—Security techniques—Information security management systems—Overview and vocabulary*. International Organization for Standardization/International Electrotechnical Commission (2005).

risk management correctly within any utility. The more unstructured and fragmented the utility asset plan and interdependencies, the more difficult this job will become. One of the key focuses in utilities security risk management may very well be the development of one consolidated and absolutely comprehensive security risk management program to guide the industry. It would find a measure of standard risk management practices that will eventually drive security requirements for entire industries.

Defining Security Risk for Utilities

Security risk and how to handle it is being redefined for utilities as it is throughout the entire security industry. Twenty years ago, security risk management consisted of assessing threats and reviewing the existing security systems in tandem with a paper-and-pen format. There have always been thought leaders in this area. The larger utilities that practiced more rigorous risk management attempted to apply a more structured process for risk assessment into the security domain, or they applied more serious threat indicators into a safety risk matrix or overall corporate risk matrix for insurance purposes. To suggest that comprehensive risk assessment drove spending decisions on security upgrades, such as those that have materialized over the past 10 to 15 years, is misrepresenting what actually occurred. Security professionals with industry-leading expertise in security risk assessment typically learned their skills and acquired their experience within a high-risk industry, like the oil industry, or within a military application, where detailed risk assessment began to move to the forefront as a tactic for assessing protection and response priorities. Such decisions were driven out of necessity and were based on more comprehensive threat assessment, vulnerability assessment, and threat agent tactical analysis. Utilities generally used a looser assessment approach to derive security mitigation measures.

A definition for risk is the likelihood of an event multiplied by its impact. To phrase it another way would be probability multiplied by consequences, or

$$R = P \times C$$

It is a simple, basic view of a risk calculation because in the ongoing science and struggle to effectively define risk, the formula can become quite large and complex. In a simple formula, however, we can begin to understand how we measure security risk for a utility.

It is why threat and vulnerability are such huge parts of risk assessment. Knowing what threats are out there is important, but knowing how these threats can impact an organization is critical in determining consequential values. Knowing how a human threat agent operates is essential in determining potential or likelihood when assessing severity. Looking at historical values is needed in assessing likelihood of an impact (once in 10,000 years, once a week, etc.).

Risk

the measure of potential damage to or loss of an asset based on the probability of an undesired occurrence

Threat

the intention and capability of an adversary to undertake actions that will be detrimental to people, the environment, assets, and economic stability

Assets

any person, facility, material, information, business reputation, or activity that has value to an operation

Source: Canadian Standards Association, Standards Z246.1-09

For utilities with numerous high-profile and high-value assets, critical infrastructure at risk, and numerous systems needed to operate complex plants and facilities, a comprehensive risk assessment that leads to effective mitigation planning needs to be conducted in many layers and with the appropriate expertise. A plant, after all, is not a singularity. It is a system of systems and people. People come in many categories, like employees (part-time, full-time, and temporary), contractors, delivery persons, and visitors, each with its own relative risk to the operation. Plants are made up of machinery, communications networks, water systems, fuel systems, sewage systems, and so on, each with its own contribution to the effective operation of the plant and each having a relative set of vulnerabilities representing different levels of impact to the organization, with threat potential. Each represents a unique opportunity for exploitation. Each must be considered in the overall assessment. This takes time, experience, and a systematic methodology to complete.

Security practitioners may be concerned about the efficacy of including natural phenomena within a security risk assessment given that this category of threat or hazard is not attack-based. However, security managers need to be as concerned about the security posture of their facility (for example, after an earthquake or tornado) in terms of vulnerability as they are over human-caused threats. Consider looting or inadvertent access to a plant after a major disaster leading to unexpected security problems, safety issues, accidental death, or plant closure as a result. When considering the foregoing, it would be helpful to discuss also the legal tort of negligent security.

What is negligent security? Negligent security cases involve the failure of companies to implement reasonable security measures for protection of their customers from crime. Negligent security case verdicts can be substantial. How does negligent security relate to the critical infrastructure sector and risk assessments? Utilities have a duty to keep customers and employees safe while on the premises. Drinking water has to be free from contaminants, power must be safe and reliable, and so forth. Suppose a criminal act or terrorist attack occurs and a hospital is without water for a significant period of time due to the attack. Assuming patients become sick as a result of the hospital not having clean water, a competent plaintiff attorney would, in the discovery phase of the lawsuit, obtain copies of all risk assessments and security measures. If the risk assessment is inadequate, outdated, or the utility did not do what it said it would in the risk assessment, then the utility could be held liable for damages. Moreover, in the current legal environment, terrorist attacks are now considered foreseeable.

Therefore, security managers should be mindful of these liability issues arising out of inadequate or outdated risk assessments, and they must make sure that the utility mitigates the risks as stated in the risk assessment. There is legal precedent that shows companies can be liable for substantial verdicts due to this oversight. For example, in the 1993 World Trade Center bombing, there were over 175 separate lawsuits, 400 claims for compensation, and a $1.8 billion verdict. The jury found that, although the risk assessment was adequate, the company had not mitigated the risk as it stated it would do in the assessment. One of the vulnerabilities stated in the risk assessment was that the World Trade Centers were vulnerable to a bomb. Therefore, a terrorist attack using a bomb was deemed foreseeable and thus preventable.

Even then, a plant assessment that considers all this must have a means for ranking assets so that vulnerability and threat can be processed realistically in terms of overall risk. A level-1 hydroelectric dam, for example, should be considered with far more priority than a level-3 dam in the overall company risk treatment. A level-1 dam

with no perimeter system would lead to a higher consequence value than a level-3 dam would. Determining what could compromise a level-1, -2, or -3 dam is an exercise unto itself. The same ranking system will apply to any asset prior to a risk assessment and typically requires a lot of input and is more apt to be associated with a business continuity and disaster recovery assessment than other forms of assessment. Security risk is not the only contributor to determining the ranking of a dam, but the issue at hand in this example relates to the terrorist threat. Additionally, the potential for business losses, societal impacts, environmental damage, and loss of reputation if the asset were to experience catastrophic consequences must be considered in an effective asset ranking. This is also true for ranking IT assets across the company. Those most critical to the company's operations will receive a higher criticality ranking and will likely be protected by a higher level of security based on threat and vulnerability.

In this more simplified view of asset ranking, a reasonable understanding of this step in the process should be clear. It is not unlike information classification, which is an added procedure that precedes a security risk assessment. Knowing the value of information that exists and moves through a company is necessary in terms of determining by what standard each piece of information should be protected. Once classified and with a standard applied, the impact or consequences of loss need to be determined through the risk assessment process. Classifying work space is also important. Determining what is public space, transition space, and confidential work space (or higher) is fundamental in placing and treating assets within the space. A risk assessment will then seek to determine whether each information asset is effectively protected to the standard required and should also then provide a listing of threats applicable to the loss of each asset and the vulnerabilities likely to be exploited in any attempt to compromise the asset. An example of work space classification is: (1) security zone; (2) operational zone; (3) reception or transition zone; and (4) public zone.

After some thorough and difficult work, it will lead to a risk summary that indicates, based on the company's priorities for risk handling, where assets need greater protection. The type and quantity of protection is determined by inspecting and evaluating the existing security program and establishing best options based on cost-effectiveness, practicality, ongoing costs to maintain security, and so forth. Mitigation for any particular risk can include a set of solutions, one single solution, or outright acceptance of the risk. Determining what is an effective security solution within the utility environment is an extensive topic by itself. Mitigating risks cannot be thought of solely in terms of fences and physical barriers. Access control itself has numerous variations. Sometimes, transferring risk is the best solution—provided transferring risk to a third party is a financial decision that can be sustained and not an attempt to avoid accountability.

Transfer of risk is not as easy a mitigation option to assess as some believe. Accountability can never be transferred. Risk assessment also needs to consider this, especially from a public safety perspective if not a life safety perspective. Protecting the corporate reputation and recovering significant financial losses is one thing, but death and related impacts will not keep the company's hands clean no matter how risk is managed. Government and safety authority inquiries can lead to significant long-term impacts for a utility. Consider just the fallout from a workplace violence event involving an active shooter and a resulting death. Society has indicated that workplace violence is avoidable and needs to be effectively managed. Failure to do so can also have criminal consequences for the company executives, who are the ultimate accountable persons when an avoidable violent

incident occurs. This will apply equally to environmental catastrophes and industrial accidents. The notion of "unforeseen" is slowly being squeezed out of the risk lexicon in modern society. Making a dollar at the expense of anyone's life or significant societal impact will result in unfavorable press. Security managers have a large role in this discussion through effective risk management practices. Transferring risk to a security guard service comes with its own risk that must be factored into the prevailing threat. Guards can impose vulnerability as well as a form of mitigation in some circumstances. Determining how much protection to apply in appropriate layers is an important part of risk treatment.

Security risk for all industrial facilities, utilities included, has met greater scrutiny by government and regulators, with regulators wanting to know that a utility is managing risk effectively. At a base level, effective security management reduces 'costs through losses' and improves rate-payer costs. Given the impact potential to utilities from terrorism, metal theft, and other forms of crime, security risk management holds a large piece of the puzzle.

Consider the potential for unintended yet peripheral consequences to something seemingly benign like the removal of copper grounds from a substation fence or the removal of communication fiber at a plant. The financial impact from the loss may not even meet a $500 loss threshold, yet the posed consequences would be at disastrous levels. Removing grounds can create an electrical hazard to workers and members of the public.

Loss of a communications cable could put a plant into shutdown or cause a loss of control for critical systems in operation at the plant. Each of these scenarios can have further downstream impacts. Let's look at our level-3 dam again and what would happen if the loss of a communications cable caused a remote dam to shut itself down, reducing water flow through the intake gates. Consider the potential for impacts on the fish stock down river—the cost of a 10 or 20 foot length of fiber could result in millions of dollars in reparation. The loss of use or generation potential of this dam may be inconsequential, yet the overall impact may not be so. Security mitigation of all risk is of importance that relies on an effective and accurate assessment.

After the events of 9/11 in particular but stemming from other incidents from decades ago, government has sought to have utilities accept greater responsibility for risk management and security program activities. This is reflected in NERC Mandatory Reliability Standards (MRS) as one example of government regulation of the electricity industry. Another more recent example would be the development of the NIST IR 7628 standard for smart grid, which is not yet regulatory but potentially destined to be. NIST IR 7628 is most certainly a government-driven initiative through the Federal Energy Regulatory Commission (FERC). One need only review existing federal and state legislation in the queue to see that governments are diligently working to introduce more comprehensive privacy laws and cyber security laws on behalf of their constituents. Debate will continue as to whether or not government regulation is appropriate or even effective in the development of basic protection standards for utilities, but there is clear evidence that industry working groups, governments, and other stakeholders are working together in pursuit of better security standards, especially as applied to IT security controls. In terms of NERC Critical Infrastructure Protection standards (NERC CIP 002–009), these critical cyber asset protection standards have almost become a default industry standard for self-regulation by virtue of the depth of industry involvement in the formulation, amendment, and management of the standards set. But the reality is FERC made NERC MRS mandatory in the United States while Canadian provinces have

accepted voluntary conformity to these standards through local regulators. The cost of such imposed standards is also widely debated and will always drive some resistance to regulatory compliance. More involvement by security experts is required to ensure compliance is focused in the priority areas of the business operations.

Most concerning to industry and security professionals may be the effects regulatory security standards will have on security itself. Opponents of government-regulated security argue that a compliance program with weighty fines for noncompliance will result in the utility managing security to avoid fines rather than managing an effective security program. After all, if a utility was to develop and manage effective security risk management on its own, one could argue that the standard driven by NERC CIP would be either contained within the utility's security program or the utility would have a security standard better than what NERC CIP requires. Thus, a self-regulated model would likely be more complete (compared to one centered on critical cyber asset), would provide additional layers of security irrespective of how cyber assets are categorized, and would, by definition, have categorized assets and prescribed many layers of security to protect them.

One can view regulatory standards as a societal response to the few utilities that were able to develop comprehensive security programs that did a good job of sustaining the good work they have implemented. Business priorities have rarely coincided with security priorities in the past. Without someone pushing hard against natural tendencies to downplay risk likelihoods and/or impacts, business drivers often bypass the cost of security. How often have we seen security applied only after a critical event? It is much too common. A very positive outcome of the NERC CIP development over the years has been the definition of security management practices relating to cyber security protection, which for the first time brought together all the elements of a protection management program necessary to sustain a security posture at the critical asset level.

This good work by industry and government has established a new benchmark for security management development. It also furthered the integration of security disciplines viewing physical and cyber security elements as necessary components of the overall program, albeit less comprehensively than is required for an overall utility security program. It was, however, sufficient to meet the criticality requirements of those cyber assets identified for critical protection. The risk assessment process defined by NERC, although not necessarily uniformly applied across all assets of all utilities, was another important step in maturing risk management within the security industry. Sometimes government has a unique way of motivating industry. One could argue this is precisely its role where society may be brought into harm's way as the result of industry failing to address prevailing risk.

More recently, the U.S. Department of Energy drafted a risk management framework for the electrical sector with, once again, a focus on critical infrastructure. The electricity sector bears considerable weight in terms of CI interdependencies. The effective recovery of the electrical grid is paramount in the recovery of other sectors and in terms of the well-being of society, generally. Once again the government focus is on cyber security. The DOE draft for public comment as of August 2011 was titled, "Electricity Sector Cybersecurity Risk Management Process Guideline" of which the version 2 draft is now complete. There are three words that should pop out from the title page, immediately. These are risk, process, and guideline, because they speak to three very important ideas relating to government, security management, and industry cooperation.

The focus of the Guideline is risk management, which is important because then it can apply to any security program regardless of whether a program pertains to physical assets, IT assets, or both. The fact that the U.S. Department of Energy seeks to develop a process to lead effective risk management is also rather important. Providing a process makes use of existing risk management processes, like ISO 30000, Australia-New Zealand 4360 (AS/NZ 4360), and even the risk assessment basis of the NERC CIP standard. So in theory, the utility would not be caught off-guard or be intimidated by the defined process. The Department of Energy offers it as a guideline, which is important because it proposes something that is presumably very meaningful in pursuit of improved security risk management but does not have the stigma of a standard or government policy, and certainly is not in the regulatory cupboard.

Given the extensive efforts by Department of Energy and its stakeholders to include and consult industry and the public on the development of this standard takes the electricity industry one step closer to self-compliance using a comprehensive tool toward this end. None of this should imply that any current guideline or standards set is the last word in security risk management. All standards require ongoing review, evaluation, and revision because the world is a dynamic organism in constant change, and so must security management assessment and practices be.

The Security Risk Management Process

Specific to the security professional within the utilities sector, resources helpful in interpretting ISO 30000 and AUS/NZ Risk Management standards should be sought when starting out. These standards provide direction for the risk management process. The process itself drives the risk management program.

Within the Canadian standards community, the Canadian Standards Association leads the effort to standardize security program management with CSA Standard Z246.1-09, Security Management for Petroleum and Natural Gas Industry Systems Government Input to Risk Management for Utilities. Section 5 of CSA Standard Z246.1-09 provides a clear process for managing security risk; detailing all of the steps required to achieve effective security risk management. In general, the process laid out includes:

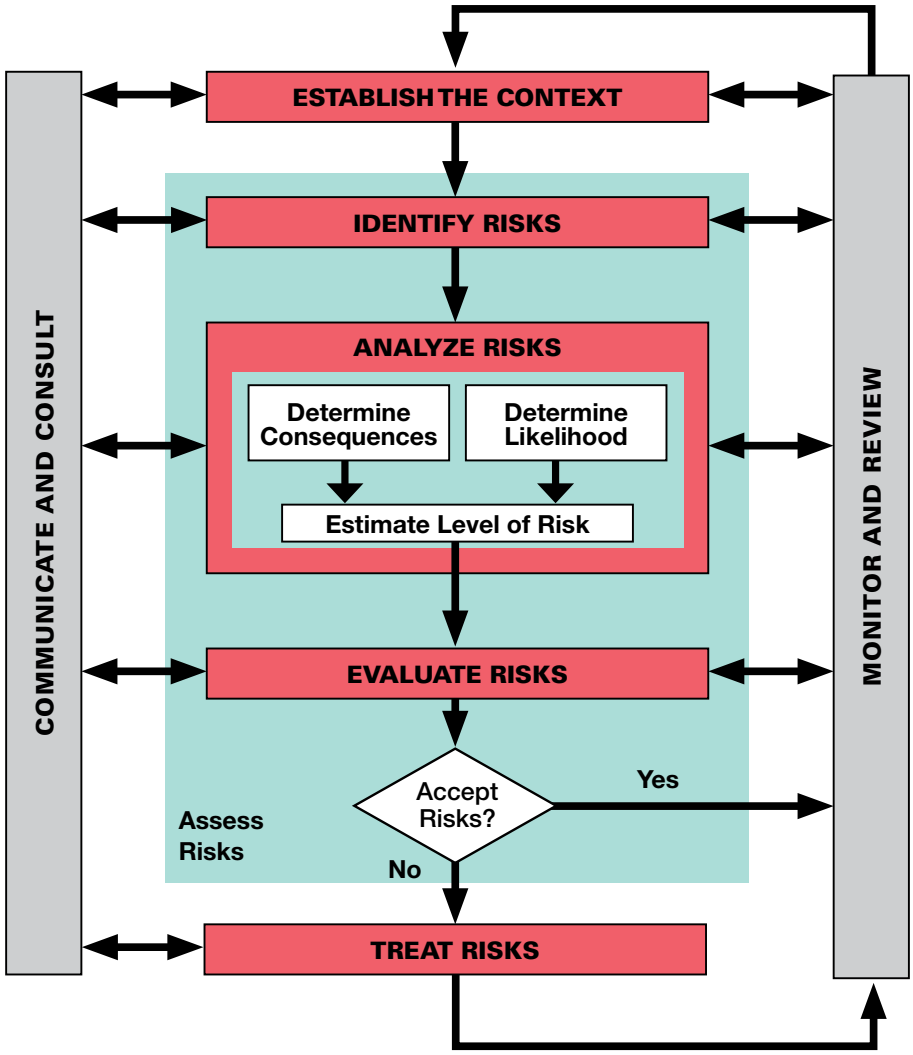
- Asset Characterization
- Threat Assessment
- Vulnerability Assessment
- Risk Assessment
- Risk Mitigation
- Communication and Recommendations

Section 5 further describes in detail how these steps are carried out. Extrapolating from this, the security management "program" which CSA246.1-09 speaks to is the extended risk management program and the assessment process the initial process in addressing risk to be mitigated through the program.

For the water sector, J-100 RAMCAP (Risk Analysis and Management for Critical Asset Protection) Methodology is the industry standard. J-100 is very similar to the aforementioned standards with the exception J-100 is SAFETY (Supporting Anti-Terrorism by Fostering Effective Technologies) Act certified, which means using the J-100 standard will protect the utility, as a matter of law, from civil liability arising from a terrorist attack.

The NERC MRS contains Critical Infrastructure Protection Standards (NERC CIP 002–009), which provide a programmatic and methodical process for managing critical cyber asset risk management, including physical security dependencies throughout the electricity transmission systems in North America. NERC established its NERC CIP standard using well-known risk management standards, already mentioned in this paper. NERC CIP, from the security perspective, then unveils a rational program for managing risk, in part through effective management processes that begin with identifying which cyber assets are critical.

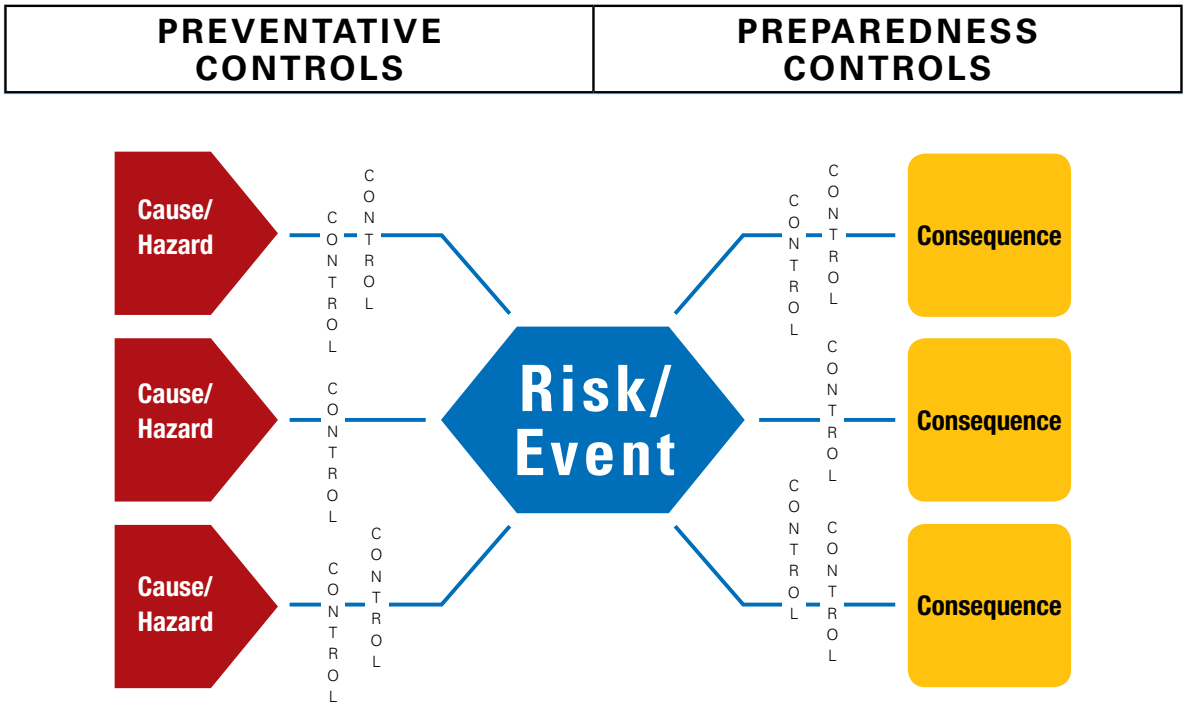
The U.S. Department of Energy in collaboration with NIST and NERC developed a Risk Management Process (RMP) designed to help utilities better assess cyber security risks. With input from FERC and DHS, this draft guideline was made available for public comments until October 2011 before going into its next iterative draft process. While specific to cyber security risk assessment, this model for RMP is no less applicable to the utility's overall security management program and, as is fitting in today's integrated security climate, very appropriate to assessing the cyber security risk across the security platform wherein IT assets both are critical to the delivery of security services (CCTV, access control) and are critical cyber assets to the overall operation of the utility (SCADA systems, energy management systems, smart grid components). This guideline effectively details what NERC CIP has always intended for transmission system critical cyber assets, then broadens the risk management process for the very complex smart grid system of systems.



AS/NZS Risk Management Process

These standards and guidelines will provide ample background for the adoption/development of a risk management process in any utility. Many others are also available and these include ISO 31000:2009 Standard and AS/NZS 4360:2004 Standard. ISO 31000:2009 was developed to replace AS/NZS 4360:2004. The Australian standard provided a methodology for risk management as a process. ISO 31000:2009 outlines an entire risk management system incorporating risk management design, implementation, maintenance, and ongoing improvements to the process. Other standards bodies and professional organizations also provide information on risk management process. All risk management processes seem to be converging into a similar format, in any event given the dominance, internationally, of the ISO standard. This is likely a positive thing. While risk analysis can be a very complex discussion, the process for managing risk should be a common platform. Ultimately, the security manager will want to ensure that the process set forth for security assessment follows the enterprise model and makes use of a common ranking system and prioritization scheme to ensure that security is treated with the same diligence and understanding as other business risk within the utility.

In this discussion, risk associated with business continuity programs, disaster recovery programs, and emergency management programs feeds into and forms part of the overall security risk. Prevention, setting barriers against unwanted events, is only one side of the equation. Responding to events that impact a utility is the other, very important half of the model.



Adapted from Reliancerisk.com.au, *Using Bow-tie Analysis to Simplify Risk Management*

IT Security Risk Management versus Physical Security Risk Management

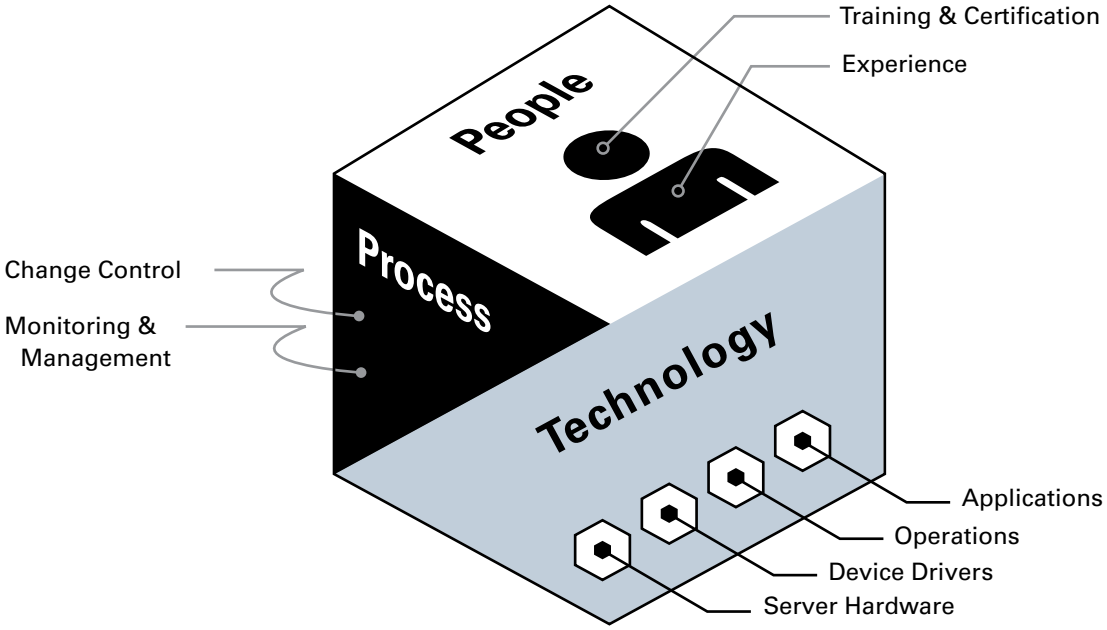
In general, there is no discernible difference in the methodology of security risk management between cyber and physical security in that both rely on approved international standards. The primary difference is in process. IT and physical security rely on threat and vulnerability assessment applied to asset criticality as key parts of the assessment, but IT risk management takes a slightly different view of vulnerability. Identifying a critical cyber asset can follow a similar methodology (as for critical dams, powerhouses, substations, etc.), but vulnerability in the IT world is based more on policy application. For example, if a password policy is not applied appropriately to a critical cyber asset, this will be flagged as a vulnerability leading to some quantifiable or qualifiable ranking of risk for the given asset. A vulnerability for a physical asset can range from lack of effective barriers (fences, gates, bollards) to lack of effective surveillance (guards, staff, video, etc.), and may not be policy related whatsoever but

rather a factor of some established standards set (usually a minimum "fencing will be used …") or protection principle (delay, detection, deterrence, CPTED, etc.). IT security practices use a very structured process for classifying risk that may be inherent to physical security risk management overall but is not categorized in the same detail. IT security, for example, looks at IT impacts in terms of people, process, and technology. This structure lends itself to categorizing threats based on their root cause categories. This is a logical view because all IT will fail as the result of one of the three or any combination of these root causes. Physical assets are typically impacted by two root cause groupings, natural causes (earthquakes, hurricanes, sand storms, geomagnetic interference, etc.) and human-caused events. Human-caused events can be intentional (malicious) or unintentional (accidental). Each of these can be broken into subcategories like biological and criminal. Within each categorization, there are multiple threats listed that need to be a considered against the health of the asset in question. The exact same process used for physical risk assessment can be applied to the IT risk assessment, but the attack vectors are very different in many cases, which implies that the assessment process must vary.

Considered in another way, physical vulnerabilities can be inherent in the structural or physical attributes of the facility—a communications system (which requires IT maintenance) may be a means to compromise a facility or could be a component of an intended assault on a facility, just as it may form part of the protection mechanism of the facility. Communications systems are the backbone of normal business operations for telephony, signaling, and IT, just as they are used to carry security alarm, video signals, and more. But mitigating the vulnerability does not rely on any physical or IT policy, per se. Enhancing security around the communications hub of a facility may rely on a detailed assessment of barriers using detection, delay, and response factors to ensure the communications hub is not immediately in play during an assault. Therefore, making use of existing or other enhanced physical security controls, such as fences, access control, perimeter security, and guards, works equally well for the communications hub (in-depth barriers) as for security vulnerabilities related to other aspects of the facility.

IT security vulnerabilities (which can include physical security features) look at the application of cyber access vulnerabilities and enhanced security options like encryption and others as the application of policy to maintain that cyber asset in a state of high security. Of course, this is an oversimplified example of cyber security, which will likely include network monitoring, patching, and other features in a comprehensive set of applied policies based on a standards set (e.g., ISO 27002) as an industry best practice. Looking back to the original statement on this, then, by looking at IT in the context of people, process, and technology, policies are categorized based on the vulnerability potential—from people, technology, or process root cause. Physical security could do something similar, but then the application of threats to the vulnerability set becomes very complex and the methodology would have to shift to allow for the much larger threat list and vast number of variables in a physical setting. Still, there is considerable maturity in the way IT security structures risk management. The cyber world, while vast and unwieldy in its structure (or lack thereof), is actually a finite set of components that make up the system. The IT aspect is a system of computers (different types), interfaces (different types), and communication networks (different types). The physical security world is far more complex, but the two have commonalities. Methodologies relating to risk assessment will benefit greatly from continued study and integration.

So it leads us to this viewpoint: Why run two different assessment processes when they feed the same enterprise risk view and rely on each other for support and operational integrity? If we change the methodology somewhat by plotting the results for treatment, can they be an integrated and shared approach? Let us take a closer look at the IT side for more granularity in our understanding of the people-process-technology (PPT) triangle.



In the realm of information technology, if all *people* within a company are enabled absolute trust by the company, then what is the organizational need for IT security? The principle basis of IT security (information system security) is the acronym CIA (or confidentiality [of data], integrity [of data], and accessibility [of data]). In other words, an IT system is not functioning if information within it cannot be maintained as confidential, reliable, and accessible. Trust comes in different degrees and compromising CIA is not only a human trust-based issue. Technology does malfunction, even without "human error" attribution, sometimes. Technology must be configured and set up appropriately from implementation. It needs maintenance and monitoring because all technology becomes out-of-date, eventually. When we speak of people and trust in the same breath on the IT side of the equation, it is not only about trusting those who have permission to access the system but extends outside the trusted domain because current technologies live in a connected environment. It can be segmented and "sandboxed" with all kinds of security in play, but it is rarely isolated in network architecture, even if there is no intention to make a particular server or application available outside the trusted domain. Therefore, applying technology correctly, ensuring the technology functions as intended, and applying processes that assure policy is managed well through the lifecycle of the technology are critical in the protection triangle. CIA and PPT are two triangles that do not intersect but which by necessity must work in unison to ensure effective IT security. CIA may apply in the physical world, but only to a small percentage of what requires protection. PPT may apply in the physical world, but it is a far more complex application of these categories than what exists for cyber security. Each by its own are extremely important in the end-to-end (E2E) utility protection umbrella. An integrated IT and physical security approach is justifiable.

Government Input to Utilities Risk Management

U.S. federal and state government interests in utility risk management has traditionally centered on maintaining and enhancing the reliability of the infrastructures that provide basic and/or necessary services to its citizens. Examples of involvement include input into NERC standards, DHS Chemical Facility Anti-Terrorism standards, EPA Water Security Initiative, FERC Security Program for Hydropower Projects, and International Atomic Energy Agency (IAEA) Nuclear Security Guidelines. Most governments believe it is their duty to intervene in business practices only when organizations are unable to meet the expectations of those they serve or if there is a belief that the utility was not providing a minimum level of safety and service required by the public. In a 2011 paper, "Law and the Social Control of American Capitalism," William Novak notes:

> They were the preeminent areas of industrial and corporate consolidation and expansion in this period (1877-1932). And they were the areas that attracted the most intense governmental interest and intervention—the unprecedented regulations that Alfred Chandler argues generated an antagonistic relationship between government and business. Indeed, to get ahead of the story just a bit, these were precisely some of the major sectors of the economy that lawyers, economists, reformers, and legislators were busily redefining as increasingly public in nature—public utilities and public services—subject to interventions ranging from increased police powers to direct rate regulation to outright public ownership.

Modern examples include HSPD-7 (Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection), which establish a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. The directive defines relevant terms and delivers 31 policy statements. These policy statements define what the directive covers and the roles various federal, state, and local agencies will play in carrying it out. HSPD-9 (Homeland Security Presidential Directive 9: Defense of United States Agriculture and Food) has a single purpose. The Attorney General, the Secretary of Homeland Security, and the Director of Central Intelligence, in coordination with the Secretaries of Agriculture, Health and Human Services, and the Administrator of the Environmental Protection Agency, develop and enhance intelligence operations and analysis capabilities within the agriculture, food, and water sectors. These intelligence capabilities include collection and analysis of information concerning threats, delivery systems, and methods that could be directed against these sectors.

State public utility commissions (PUCs) are another regulatory body created to best serve the interests of utility customers. From the Colorado PUC's website:

> The Colorado Public Utilities Commission serves the public interest by effectively regulating utilities and facilities so that the people of Colorado receive safe, reliable, and reasonably-priced services consistent with the economic, environmental and social values of our state.

This normally is felt through standards, guidelines, and service level requirements, including penalties. Standards and guidelines are usually developed as a result of lessons learned from service interruption incidents – rarely are they developed with forethought, except for the North American Electric Reliability Corporation (NERC) cyber security standards. These standards were developed as a pre-emptive effort to protect the bulk electric grid from known and perceived cyber threats.

Penalties may be levied on organizations that do not comply with federal standards or state requirements through their utility commissions for organizations they regulate for not meeting their service level requirements. Note that the PUC's statement in this case does not specifically refer to effective risk management process, but inevitably the application of standards and guidelines cannot be done in a meaningful way unless assessment is completed first. The PUC does state, correctly, that the application of standards is preemptive, or preventative (remember the bow tie model?) in the grid protection model.

One of the primary foundations for any security department of an electric utility that contributes to the U.S. bulk power system is the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) cyber security standards. As previously discussed, NERC CIP provides both, a standard for protection through security program management and a methodology for managing security risk. These, too, go hand in hand.

NERC Historical Background

Given the prominence of NERC as an electricity sector regulator and author of one of the first critical infrastructure dependant standards for security in the world, it is important to have a more granular look at this organization in terms of its formation, approach, and scope to risk management. NERC CIPs have been discussed extensively in terms of achieving industry standards adoption, and will be used as a model for further additional standards regulation being considered.

The National Electric Reliability Council (NERC, name changed in 1981 to the North American Electric Reliability Corporation when Canadian electric companies voluntarily joined the organization) was established June 1, 1968, by the electric utility industry in response to the 1965 Northeast blackout. 30 million people lost power for up to 13 hours. The organization was created and funded by the voluntary participation of electric utility organizations that provided the generation, transmission, and distribution of electric power. Twelve regional reliability organizations were formalized, reporting to NERC. The current eight regional entities include

- FRCC - Florida Reliability Coordinating Council
- MRO - Midwest Reliability Organization
- NPCC - Northeast Power Coordinating Council
- RFC - Reliability First Corporation
- SERC - SERC Reliability Corporation
- SPP - Southwest Power Pool
- TRE - Texas Regional Entity
- WECC - Western Electricity Coordinating Council

The Alaska Systems Coordinating Council (ASCC) is an affiliate NERC member.

On August 14, 2003, a larger blackout occurred in the Northeast and Midwest, which affected over 50 million people. That event propelled NERC to convert its operating policies, planning standards, and compliance requirements into an integrated and comprehensive set of 90 measurable standards called "Version 0 Reliability Standards" on November 12, 2004. Those reliability standards went into effect April 1, 2005. Voluntary compliance was expected as a matter of good utility practice. In August of 2005, the U.S. Energy Policy Act of 2005 was signed into law, authorizing the creation of a self-regulatory electric reliability organization (ERO) that would span North America, with Federal Energy Regulatory Commission (FERC) oversight in the United States. NERC became the ERO on July 20, 2006, and changed from a council to a corporation in 2007. In March 2007, FERC approved 83 NERC Reliability Standards, the first set of legally enforceable standards for the U.S. bulk power system, effective June 4, 2007. On June 18, 2007, compliance with approved NERC Reliability Standards became mandatory and enforceable in the United States.

The standards set consists of nine divisions, CIP-002 through CIP-009 cyber security standards plus a suspicious incident reporting requirement, CIP-001. NERC CIP standards are currently in version 4 and 4/5. The standards have been evolving continually since their creation, with version 4 adopted by the NERC Board of Trustees February 9, 2012, and version 5 in review. The cyber security standards were created based on NERC member companies' best practices utilizing the American National Standards Institute (ANSI) standards development process. The process to create these standards is guided by the institute's cardinal principles of consensus, due process, and openness, which depends heavily upon data gathering and compromises among a diverse range of stakeholders. Each day the cyber and physical security departments of electric utilities adhere to the standard and document their compliance.

The relationship is mutual. Standards bodies will continue support of NERC working group efforts as long as NERC supports NIST and other standards bodies. Many members of NERC working groups also sit on standards bodies working groups.

Smart Grid View

Similar efforts are underway to find a set of "reliability standards" that can be applied to the smart grid, a far more complex machine than the standard transmission model covered by NERC MRS. As of this writing, FERC has accepted one initial draft submission by NIST in the form of NISTIR 7628 (*Interagency Report 7628, Guidelines for Smart Grid Cyber Security*). Provided in three volumes—"Architecture and Requirements", "Risk Management", and "Supportive Analyses and References"—they form the closest reference set for smart grid security standardization available today. NISTIR 7628 is the product of a wholly collaborative and open process led by the Smart Grid Interoperability Panel's Cyber Security Working Group.

The aforementioned U.S. Department of Energy guideline, *Electricity Sector Cyber Security Risk Management Process Guideline*, is another integral component to the efforts to standardize security practices for utilities in the development of smart grid. It seems apparent that industry is a major player in the formulation of a guideline, and it is equally apparent that standardized risk assessment is a means to avoid NERC CIP-style mandatory regulations imposed by government on utilities. The future view of this is still uncertain. The final form and application of NISTIR 7628, the DOE Security Risk Management Process Guideline, or any future guideline or standards set will be determined by a number of factors. These include prevailing national threats, utilities adoption of effective standards, and some form of self-regulation being in place. Additionally, factors such as the size and complexity of the growing grid and the practicality of applying any form of mandatory standards beyond some basic core set as a management practice will influence this discussion.

The application of a standardized risk management process appears to be an important step in achieving a foundational and integral component of security standards application to the smart grid in addition to all other facets of the utility operations. To date the majority of the discussion about smart grid vulnerabilities has been a view from the outside using various threat vectors within the smart grid to address critical cyber systems (e.g., SCADA) or breaches in customer confidentiality. What is not discussed is the potential to compromise legacy systems within the utility to do the same thing, including impacting the smart grid. Eventually standards sets may need to address the entire utility and its interoperable environment and not limit themselves to the new smart grid technology and its interfaces with legacy IT. The risk management approach would need to be far more holistic, inclusive, and should be contemplated and applied from a strict governance, risk, and compliance perspective (GRC). Just like people, process, and technology, GRC cannot be broken into independent parts of focus. Each is interdependent.

Risk Management Tools

The correct tool(s) to use depends on the type of risk assessment methodology applied. This paper has discussed primarily a standards approach to risk management that applies risk as probability of an event multiplied by the impact of the event on the asset or operation. We measure threat, vulnerability, and consequences in this calculation in a comprehensive manner. In a utility environment, other forms of assessments are applicable and this includes root cause analysis, which is very complex, time-consuming, and requires considerable collaboration and expertise to perform correctly. There are few experts in root cause analysis who can perform these assessments to the degree of exactness needed. Excerpted from the Wikipedia article on root cause analysis (RCA):

1. The primary aim of RCA is to identify the factors that resulted in the nature, the magnitude, the location, and the timing of the harmful outcomes (consequences) of one or more past events in order to identify what behaviors, actions, inactions, or conditions need to be changed to prevent recurrence of similar harmful outcomes and to identify the lessons to be learned to promote the achievement of better consequences. ("Success" is defined as the near-certain prevention of recurrence.)
2. To be effective, RCA must be performed systematically, usually as part of an investigation, with conclusions and root causes identified backed up by documented evidence. Usually a team effort is required.
3. There may be more than one root cause for an event or a problem, the difficult part is demonstrating the persistence and sustaining the effort required to develop them.
4. The purpose of identifying all solutions to a problem is to prevent recurrence at lowest cost in the simplest way. If there are alternatives that are equally effective, then the simplest or lowest cost approach is preferred.
5. Root causes identified depend on the way in which the problem or event is defined. Effective problem statements and event descriptions (as failures, for example) are helpful, or even required.
6. To be effective, the analysis should establish a sequence of events or timeline to understand the relationships between contributory (causal) factors, root cause(s) and the defined problem or event to prevent in the future.
7. Root cause analysis can help to transform a reactive culture (that reacts to problems) into a forward-looking culture that solves problems before they occur or escalate. More importantly, it reduces the frequency of problems occurring over time within the environment where the RCA process is used.
8. RCA is a threat to many cultures and environments. Threats to cultures often met with resistance. There may be other forms of management support required to achieve RCA effectiveness and success. For example, a "non-punitory" policy towards problem identifiers may be required.

Root cause analysis seeks to predict through a meticulous Boolean algebraic-style process the possible and probable adverse outcome precipitated from various initiating events and sequences. Done correctly, this form of analysis is one of the purest scientific methodologies available for risk management to determine, isolate, and treat threats, with a focus on single points of failure. Redundancy can be a security mitigation except where there are multiple, simultaneous attack vectors. What root cause analysis does not render is the risk measurement or ranking that allows other business processes to take hold and prioritize security risk. This makes root cause analysis a better resource to deal with safety-type hazards than security threats. One can argue, though, that any single point of failure is itself a prioritization scale; especially in an environment where the threat or hazard has already been ranked (for example, death is unacceptable; multiple fatalities are even more unacceptable).

"Best-of-breed" tools are readily available that provide enterprise risk management solutions. It is never advisable, however, to apply any security tool for any reason without sufficient research, references, experienced analysis,

oversight, and careful thought. This paper does not seek to promote or give preference to any single product. Rather, in specifying current solutions, we acknowledge they were tested and found to be reliable in terms of methodology, completeness, and effective measurement against best practices and standards in order to provide a usable risk assessment output (report) at the end of the process. With this in mind, products that provide a good comparison point when searching for a risk assessment product (especially an automated one) include Asvaco™ risk assessments on the physical side, and Modulo® and Archer™ on the IT side. Asvaco as a physical security tool is vastly different from the IT counterpart in its use and application, but it does consider the physical protection of IT.

These tools are not exclusive to the risk assessment market. Each showed good general evaluative and adaptability strengths, but each can just as easily not fit a particular enterprise or need. Understanding them will allow the security professional to move forward in assessing others. Sometimes the product is not the real need but produces expertise in applying the assessment methodology. In that case, consulting services with a strong lineage in risk assessment is most needed and typically comes with the methodology these products provide. As a general rule of thumb, the larger the utility or enterprise and the greater the number of assets, the stronger the business case for purchasing the tool. As with any significant software purchase, strong procurement practices are needed to assess the tool and to bring it into practice. This can take several months if done correctly, especially in terms of the training needed to apply the tool correctly.

From time to time, variations on pen-and-paper assessments surface; generally expansions into spreadsheet applications for self-assessment purposes. They rely on experience and personal knowledge of the assessor to be of significant value, but these should not be used except for a simple, tier-1 approach to assessment. Pen-and-paper tests lack the particulars to handle the detailed variations in utilities security standards and requirements, and do not provide the experience needed in assessing a multi-layered vulnerability environment. They do not render detailed outcomes measured against meaningful standards sets. Pen-and-paper tests are never done against an IT environment without some form of engine to handle the risk quantification algorithms. What you put into the assessment determines the usefulness of the resulting data output in the end. In the view of this paper, if a meaningful standards set is not in play as part of the measurement process and useful mathematics are not driving the risk rankings, then the assessment is little more than a filtering process that brings the security professional back to a set of decision-making steps to figure out what needs to be mitigated, what is a priority, and how treatment needs to be applied. With standards and rankings in play, this becomes either very obvious or, at the very least, provides a method for applying company priorities to the computer-generated results. With a comprehensive methodology in play, there is much less of a likelihood in missing some aspect during the assessment that could later be exploited.

Finally, it is important to consider ASIS International when seeking the tools and skills used in security risk management. The ASIS Store, with an extensive catalog, carries a number of textbooks on this topic. The ASIS membership roster consists of many security professionals who have been actively assessing security risk and managing security risk for decades. Networking with them will always lead to another suggestion. Attending ASIS conferences, especially the Annual Seminar and Exhibits, provides the best opportunity to meet fellow security professionals face to face and learn from many of the most gifted and experienced in the field. The ASIS conferences and programs also provide direct access to security vendors and consultants who will provide options for addressing risk and risk management.

Security Risk Management and Enterprise Risk Management

The enterprise risk management team within a utility will look to:

- aggregate key risks across the company and provide Key Risk Indicator (KRI) reporting;
- develop standard language and guidelines for risk management, which includes risk assessment, evaluation, treatment, and communication;
- build knowledge of risk management practices through engaging risk expertise across business groups and information exchange;
- maintain the Corporate Risk Matrix;
- review individual risk issues;
- lead a Risk Management Committee to ensure appropriate and broad focus on risk, and to provide advice to executives on key risk issues; and
- provide general risk management consulting services across the enterprise.

Enterprise risk management sets the tone and standard for risk management (including the assessment and treatment process) and manages communication and consultation on all risk issues (including key reports on risk that may require the attention of the risk management committee or executive sign-off). The aggregation of key risk is an important component of the ERM team function because the way risk is ranked over the entire enterprise often determines whether funding is made available to deal with the risk and whether specific risks receive the appropriate attention. A risk that is not appropriately ranked corporately may be accepted (in which no action will be taken towards mitigating it) and, if it was more critical than assessed, could create a major problem for the company at a later date. It is difficult to believe, for example, that some of the major oil spill episodes in the past decade were never assessed as risks to their respective companies. And, if categorized appropriately within the risk matrix, it is difficult to believe that these risks would not have been appropriately treated so as to avoid the massive environmental destruction that resulted from these incidents that ensued. Surely the end result of these incidents and the billions of dollars involved in settling damages caused by them were not deemed acceptable to go untreated. However on the same basis, risk so massive is often transferred and covered by insurance, which played a part in easing some of the pain of these oil companies. In such instances, reputational risk is easier to accept than letting the business go bankrupt. Nonetheless, the reputational damage alone would seem to have been so adverse that the company might be compelled to do more to ensure these spills were far less likely to occur. Risk tolerance also shifts corporately over time as public and government issues shift. This does not change methodology for risk management; it simply affects how risk issues will be treated. Risk assessment, as a matter of process and a matter of record, needs to remain comprehensive and an effective business control for the company and the enterprise.

$f \geq 10^{2}$	At least 100 times every year	L9	3	4	5	6	6	6	6	6
$10^{1} \leq f < 10^{2}$	At least 10 times every year	L8	3	3	4	5	6	6	6	6
$10^{0} \leq f < 10^{1}$	At least once every year	L7	2	3	3	4	5	6	6	6
$10^{-1} \leq f < 10^{-2}$	At least once every 10 years	L6	2	2	3	3	4	5	6	6
$10^{-2} \leq f < 10^{-3}$	At least once every 100 years	L5	1	1	2	3	3	4	5	6
$10^{-3} \leq f < 10^{-4}$	At least once every 1,000 years	L4	1	1	1	2	3	4	5	6
$10^{-4} \leq f < 10^{-3}$	At least once every 10,000 years	L3	1	1	1	2	2	3	4	6
$10^{-5} \leq f < 10^{-4}$	At least once every 100,000 years	L2	1	1	1	2	2	3	4	6
$10^{-6} \leq f < 10^{-5}$	At least once every 1,000,000 years	L1	1	1	1	1	2	2	3	6
$f < 10^{-6}$	Less than once every 1,000,000 years	L0	1	1	1	1	1	1	2	6

Consequence Type		Consequence Severity							
		S0	S1	S2	S3	S4	S5	S6	S7
Safety	Worker	Near Miss	First Aid	Treatment by Medical Professional	Temporary Disability	Permanent Disability	Fatality	Multiple Fatalities	
	Public	None	Near Miss	First Aid	Treatment by Medical Professional	Temporary Disability	Permanent Disability	Fatality	Multiple Fatalities
Environmental		Almost zero impact	Low impact	Moderate impact	Moderate to high impact	High impact	Very high impact	Extreme impact	
Financial		< $10K	$10K to $100K	$100k to $1M	$1M to $10M	$10M to $100M	$100M to $1B	$1B to $10B	> $10B
Reputational		None	Limited complaints to company or shareholder	Negative local profile	Small but vocal minority of customers critical	Many customers critical	Loss of trust-strategic change imposed by regulator and/or shareholder	Loss of consent to operate	
Reliability	Worker	N/A	N/A	N/A	Require voluntary load reduction	Localized load shedding	Significant load shedding required	Load shedding spreads to WECC	
	Public	None	< 5K customer hours lost per event	5K to 50K customer hours lost per event	50K to 500K customer hours lost per event	500K to 5M customer hours lost per event	5M to 50M customer hours lost per event	50M to 500M customer hours lost per event	> 500M customer hours lost per event

– courtesy British Columbia Hydro

When considering the security risk matrix, an important aspect of representing risk in this way is to not simply define each and every risk important to the utility and visually plot it across the business group or enterprise, but to quantify risk information whenever possible so that relative risk can be discerned more readily. All risk measurements are subjective in terms of how it is quantified or qualified by whom and for whom. Assigning a value (as was done in the risk matrix) as opposed to a qualifier like "high", "medium", or "low" risk adds significance. This is equally true for qualification in a threat environment indicator like green, blue, yellow, red. The matrix in our example defines risk quantification with meaningful indicators that a company can use in both the frequency and the consequence values.

Some risk assessment methodologies ask for three products to derive the risk (R) value. The risk formula, R = P x C, was presented early in this document. Often a third factor, relevance, is added. For example, spam advertising may impact a utility's email server 30 times per day and have some consequence, but it may not be relevant to the company because its email server is fully redundant and operations would not be affected if one or more servers cease functioning properly in a denial of service attack. So, the relevance of this problem that can appear to be high risk would lead to a very low risk ranking in this utility. In the matrix example, relevance is built into the numeric indicators across all columns. We can see how each numeric indicator is defined so we understand the relevance to the company. Relevance does have to be factored into a risk equation in some way. Often it can be normalized to a factor of 1 (it impacts us) or 0 (it has no impact). This will vary depending on the asset or process measured.

Summary

Knowing how risk management fits into the security program is of utmost importance. In order to apply security risk management appropriately to any utility, security managers have an understanding of the driving risk management work and risk treatment efforts. These can be related to regulatory issues or pressing social issues, major events impacting the utility, and emerging threats. Changes to the enterprise, such as mergers, acquisitions, and major domestic and international developments require careful risk assessment work. In order to ensure risk is effectively managed, the utility security manager understand how risk assessment is carried out and be familiar with risk assessment standards. Programs for risk assessment must be developed and the appropriate resources and expertise applied. Developing the risk management process requires collaboration with the utility enterprise risk group and others to ensure a cohesive company approach and common methodology. Risk assessment methodologies change slightly for safety, information technology, and physical security assessment, but each has commonalities that the other can relate to and borrow from. Ultimately, risk must be quantified or qualified to a company risk matrix or register to ensure security risk priorities are measured against and receive the same prioritization as other business risk. It is also important to understand that security risk often contributes to other company priorities. Financial losses, reputational losses, safety issues, and environmental issues all occur within the sphere of security incident impacts.

Risk assessment tools vary and require extensive research and qualification before they are applied to the utility. There are a few key, known risk assessment products that can be used as a starting point when looking at preferred features for assessment methodology and reporting types. Managing the work of an assessment is as important as performing the assessment. Risk must be ranked, prioritized, and treated. There are elements to a risk assessment that is recursive, and historical data is important for when subsequent assessments are performed. Continued high risk rankings for any asset in subsequent assessments demonstrates a problem in either prioritization or treatment. Once identified on the corporate register, risk must be treated in some way. The security manager, steward of security risk, is ultimately responsible for effective mitigation.

Eventually, the security department seeks to manage its risk like any other department in the company. Because security risk is not isolated and has impacts on many aspects of the company, it should be treated through effective barriers and programs that have company-wide reach. What comprises an effective mitigation to any risk item is subject to additional analysis like business case and ROI analysis. Additional expertise is always applied to risk treatment to ensure that the best solution is being applied to meet the assessed risk. With an effective risk management tool, using automation, sometimes the threat and vulnerability will help to drive out a recommended solution within the risk report. This is probably more true for an IT-based assessment, given that the physical assessment has many more variables. Applied expertise in preparing any engineered solutions is very important. Security resource application, security program formation, and effective solutions are driven by effective security risk management. Without it, utility security becomes something akin to guesswork, and that will not demonstrate good, long-term solutions for the utility. As risk management becomes very complex, as in a smart grid environment, risk management must adapt.

Physical and IT security have many risk dependencies and need to be measured in concert, even if it is not possible to apply the same tool to both. Physical attributes of the company rely on IT backbones, and IT assets require strong physical security measures. Determining the criticality of each asset and applying security in the correct degree treats risk most effectively. Integrating the IT and physical security view in risk assessment requires that all assets be assessed equally and in an end-to-end view showing interdependencies. This also includes applying IT security risk assessment to the security solution, including video networks and servers, access control assets, and alarm management systems. IT risk includes the manner in which servers and networks are maintained and applies equally to those security applications that are being built to protect the IT assets. Perhaps in this case the criticality is even higher.

As a final word, given the world is ever changing, risk management must by dynamic, continuous, and sustainable to be completely useful. Security risk assessments are foundational to the security management program. Having enough accurate information to apply the correct resources, management, and priority is key to a security program's success. Significant risk will be removed from the utility register when assessments are performed well. Security is not a peripheral risk concern to the utility—it is fundamental.

1625 Prince Street
Alexandria, VA 22314-2818
USA
Phone: +1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org