Cyber Security Risk Management and Risk Assessment Methodology Template

Annabelle Lee

Chief Cyber Security Specialist

Nevermore Security

December 2019

ACKNOWLEDGMENT

This document was developed under a contract to the United States Energy Association (USEA). The author acknowledges the contributions and suggestions from the Black Sea and Balkan transmission and distribution utilities. Their participation in the Utility Cyber Security Initiative (UCSI) and their input has been valuable in ensuring that the content meets their specific requirements in addressing cyber security risks.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 RISK MANAGEMENT OVERVIEW

The current power grid consists of both legacy and next generation technologies. These new components operate in conjunction with legacy equipment that may be several decades old and provide no cyber security controls. In addition, industrial control systems/supervisory control and data acquisition (ICS/SCADA) systems were originally isolated from the outside world. Sensors would monitor equipment and provide that information to a control room center. As networking technology has advanced and become more accessible, organizations have made decisions to integrate systems. This integration is necessary to take advantage of the new technology that is being deployed. With the increase in the use of digital devices and more advanced communications and information technology (IT), the overall attack surface has increased.

Cyber security must address deliberate attacks launched by disgruntled employees and nation states as well as non-malicious cyber security events such as user errors. Because organizations, including utilities, do not have unlimited resources such as personnel and funds, cyber security must be prioritized with the other components of enterprise risk. *Risk* is the potential for an unwanted impact resulting from an event. Cyber security risk is one component of enterprise risk management, which addresses many types of risk (e.g., financial, mission, public perception).

In addition, to adequately address potential threats and vulnerabilities, cyber security must be included in all phases of the system development life cycle, from the design phase through implementation, operations and maintenance, and disposition/sunset. Cyber security must be constantly assessed and revised to address evolving threats, vulnerabilities, and security incidents.

The purpose of this document is to specify a risk management and risk assessment template that may be used by utilities. This also includes the selection and tailoring of cyber security requirements and measures/controls. This document is NOT an attempt to develop new guidance but rather document the diverse existing guidance that is applicable to the electric sector.

1.1 Risk Management Overview

The process of evaluating and selecting effective risk management activities generates information that can be used during incident response to help inform decisions regarding operations restoration. It also provides the basis for understanding potential risk mitigation benefits that are used in making planning and resource decisions.

Risk management actions include measures designed to:

- Deter, disrupt, and prepare for threats
- Reduce vulnerability to an attack or other disaster
- Mitigate consequences and
- Enable timely, efficient response and restoration in a post-event situation.

The risk management approach focuses attention on prevention, protection, mitigation, response, and recovery activities that bring the greatest return on investment, not simply the

vulnerability reduction to be achieved. It is better to build security and resilience into assets, systems, and networks than to retrofit them after initial development and deployment. Accordingly, utilities should consider how risk management, robustness, and appropriate cyber security enhancements can be incorporated into design and construction, rather than "bolted on" later.

Risk management decisions should be made based on an analysis of the costs and other impacts, as well as the projected benefits of identified courses of action - including the no-action alternative if a risk is considered to be effectively managed already. When evaluating risk management options, utilities should consider industry standards and best practices and lessons learned from events and exercises. Risk management options should be described in enough detail to define the extent to which they will reduce risk. The life-cycle costs of each option should be estimated (e.g., initial investment or startup, operation and maintenance). Also, a mitigation strategy may be used across multiple attack scenarios.

Cyber security risk is only one type of risk that all utilities address. There are many other types of risk and some are illustrated in Figure 1 below.

Figure 1[1]: The Larger Risk Management System

1.2 Risk Management Process[2]

Figure 2 below illustrates a general risk management process, as defined by the SANS Institute. The diagram includes the high level steps in risk management. The figures and descriptions in the remainder of section 1 and in Section 2 expand upon this generic diagram.

---

[1] This figure is extracted from a briefing presented by Jason Christopher, Chief Technology Officer, Axio Global, Inc. Jason is currently the Principal Cyber Risk Advisor, Dragos, Inc.

[2] This section was extracted from: *Rick Management in Practice: A Guide for the Electric Sector.* EPRI, Palo Alto, CA: 2014. 30020033.

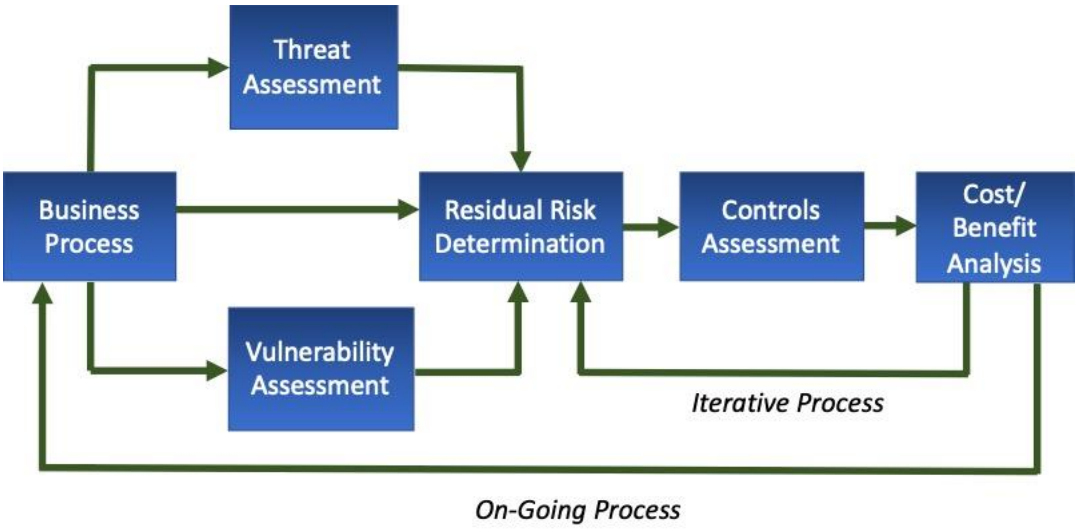

Figure 2: SANS Risk Management Process

Figure 3 below expands upon the relationship between threat, vulnerabilities, and risk management. The vulnerability management process addresses day-to-day vulnerabilities and provides input to the risk management process. The threat management process addresses day-to-day threat discoveries, provides input to the risk management process and information to update the risk criteria and taxonomy. The risk management process should continually identify, analyze, address, monitor, and report risks.

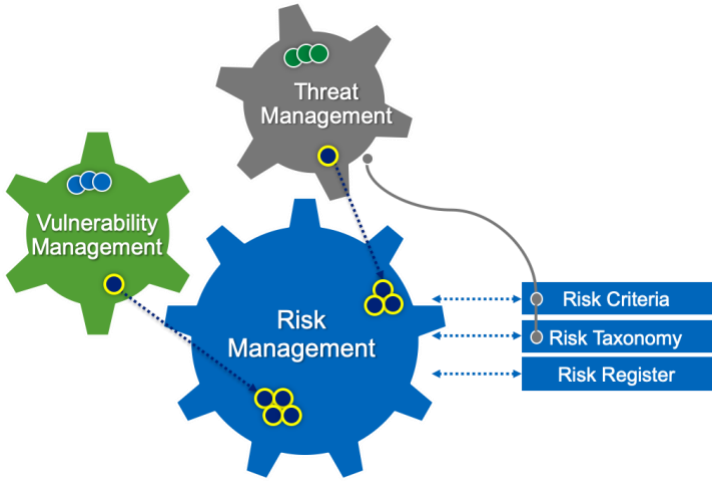

Figure 3[3]: Risk Management Component

[3] This figure and the text are extracted from a briefing presented at the November 2019 UCSI meetings by Jason Christopher, Chief Technology Officer, Axio Global, Inc. Jason is currently the Principal Cyber Risk Advisor, Dragos, Inc.

1.3 Utility Risk Management Framework

Figure 4 below builds upon the SANS process and provides an overview of a utility risk management framework and strategy and the security methodologies that may be used to implement this framework. Listed below the diagram is a description of each of the elements of the diagram and the three methodologies used in selecting and assessing security controls (maturity model, control-based, and compliance).

Included in the figure are three risk strategies, and one is cyber security. As described above, there are many types of risk that each utility addresses, and those included in the figure are not intended to be comprehensive.

- *Financial Risk Strategy* – This assesses the financial implications of adverse events, including cyber security events.

- *Mission Risk Strategy* –This looks at the risk that any failure will render a utility unable to safely deliver power.

- *Cyber Security Risk Strategy* – This looks at the impacts of cyber security compromises.

These three strategies are related – the risk of compromise of the information, business, and operational systems drive financial and mission risk, and the utility's strategy related to financial and mission risk should be a factor in setting targets and requirements for cyber security risk.

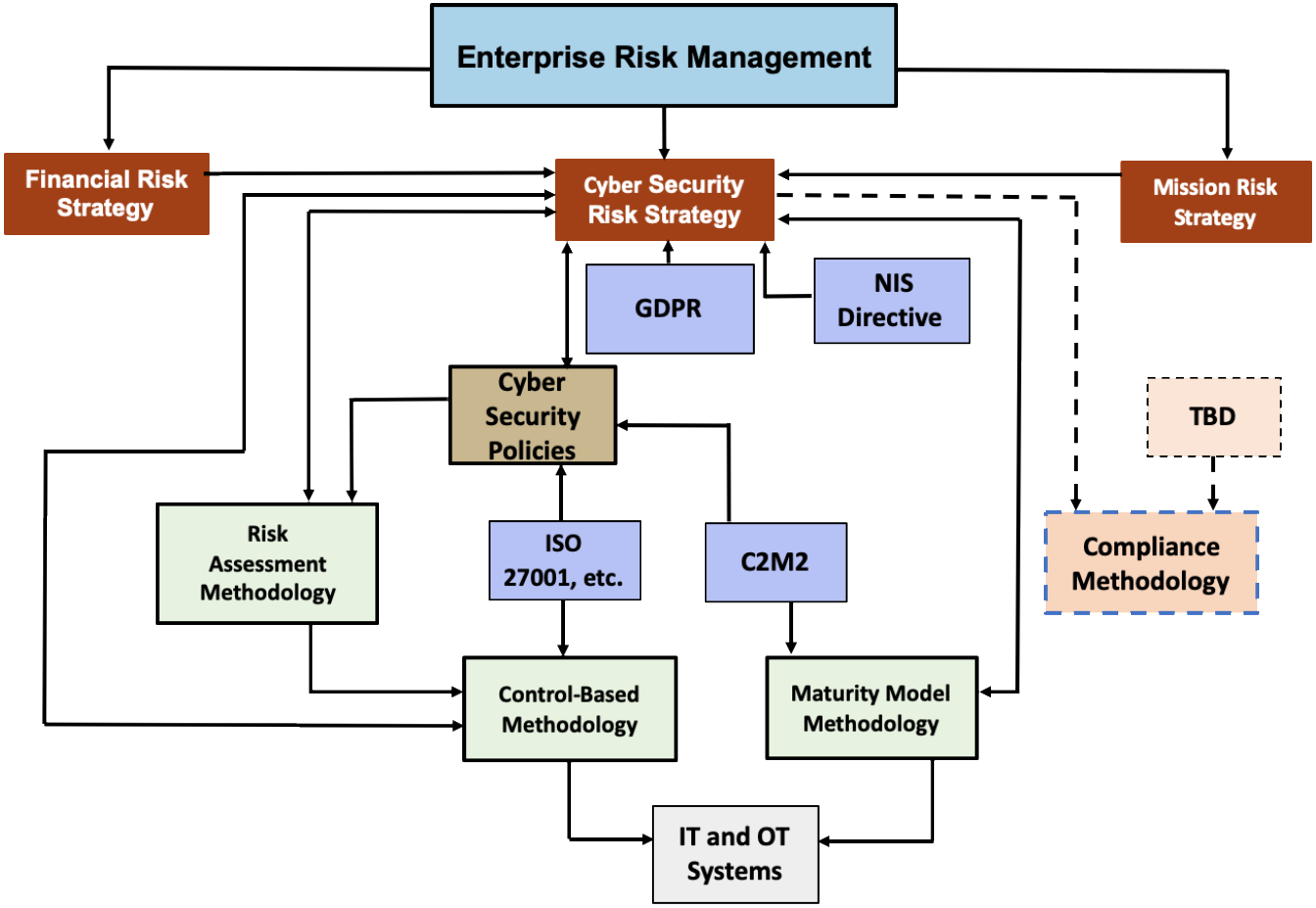

Figure 4: Utility Risk Management Framework

Acronyms:

- C2M2: Cybersecurity Capability Maturity Model
- GDPR: General Data Protection Regulation
- NIS Directive: The Directive on Security of Network and Information Systems

The cyber security risk strategy is divided into three categories based on the methodology:

- *Maturity Model Methodology* – maturity models provide utilities with a method to assess the degree of an organization's alignment with the best practices in the structure and operation of the organization and its information technology (IT) and operational technology (OT) systems. The maturity model methodology uses the C2M2 document and the C2M2 toolkit in the assessment.

- *Control-Based Methodology* – Controls based methodologies address the technical aspects related to the configuration of the IT and OT systems and protective hardware and software. The control-based methodology uses ISO 27001, and a risk assessment methodology that may be specific to the utility, or publicly available.

- *Compliance Methodology* – Compliance methodologies focus on specific mandatory requirements. Though the starting point is rules, the compliance methodology must necessarily be extended to control-level requirements. At this time, there are only regulations for the bulk electric systems. Currently, there are no regulations specific to the electric sector.

1.4 Tips in Developing a Risk Management Framework[4]

Following are tips that may be used in developing a risk management framework.

1. There is no single cyber security risk management framework that is applicable to every utility and system. There are several high level frameworks that may be used.
2. The top-level cyber security risk management framework should be at a fairly high level, to limit the requirement for constantly updating the framework.
3. When selecting a cyber security risk management framework, start by reviewing what is currently available in the utility, typically for the IT and communication systems. It is much easier to apply and/or tailor an existing framework, than to develop one from the beginning.
4. Developing or tailoring a cyber security risk management framework and identifying systems requires time and patience.
5. To perform a risk assessment, each utility needs to identify the systems. There is no single list of systems that is applicable across all utilities – each utility must develop its own list.
6. The definition of a *system* is determined by the utility but should consist of a common set of functions. In general, one system is too few and 2000 is probably too many. Defining a system is critical to the accuracy of the risk assessment, the definition of the security requirements, and the selection of cyber security controls/mitigation strategies that address the identified vulnerabilities and threats.

[4] This section was extracted from *Cyber Security Strategy Guidance for the Electric Sector*, EPRI, Palo Alto, CA: 2012. 1025672, and revised.

7. Electric sector use cases are a valuable tool that may be used in documenting functionality and identifying systems. Typically, these use cases do not focus on cyber security. There are several thousand use cases available.
8. The phases in the framework may need to be repeated. For example, in identifying systems, a utility may realize that their initial list did not sufficiently differentiate functionality.

2 RISK ASSESSMENT METHODOLOGY

The results of risk assessments inform the selection and implementation of mitigation activities and the establishment of risk management priorities for utilities. These activities help to focus planning, increase coordination, and support effective resource allocation and incident management decisions. Comparing and prioritizing the risks helps identify where risk mitigation is most needed and determines and helps justify the selection of the most cost-effective risk management options. This supports resource allocation decisions (such as where risk management programs should be instituted), guides investments in these programs, and highlights the measures that offer the greatest return on investment.

A cyber security risk assessment includes identifying assets, vulnerabilities, and threats and specifying impacts. The output is the basis for the selection of security requirements and subsequent risk-mitigation strategies (security measures/controls). This includes both malicious and non-malicious cyber security events. Non-malicious cyber security events include user errors and mis-configurations.

The risk assessment methodology should be[5]:

- **Documented:** The methodology and the assessment must clearly document what information is used and how it is analyzed to generate a risk estimate.
    - Any assumptions and decisions need to be documented and available to the user of the methodology
- **Reproducible:** The methodology must produce comparable, repeatable results. This is important when prioritizing the systems and the various risks, vulnerabilities, and impacts.
- **Defensible:** The results of the risk assessment must be documented. This information may be used when assessing the risk decisions.

Figure 5 below illustrates a risk assessment process that may be used during the system design phase.

[5] Extracted from: *NIPP Supplemental Tool Executing a Critical Infrastructure Risk Management Approach*, DHS, 2013.

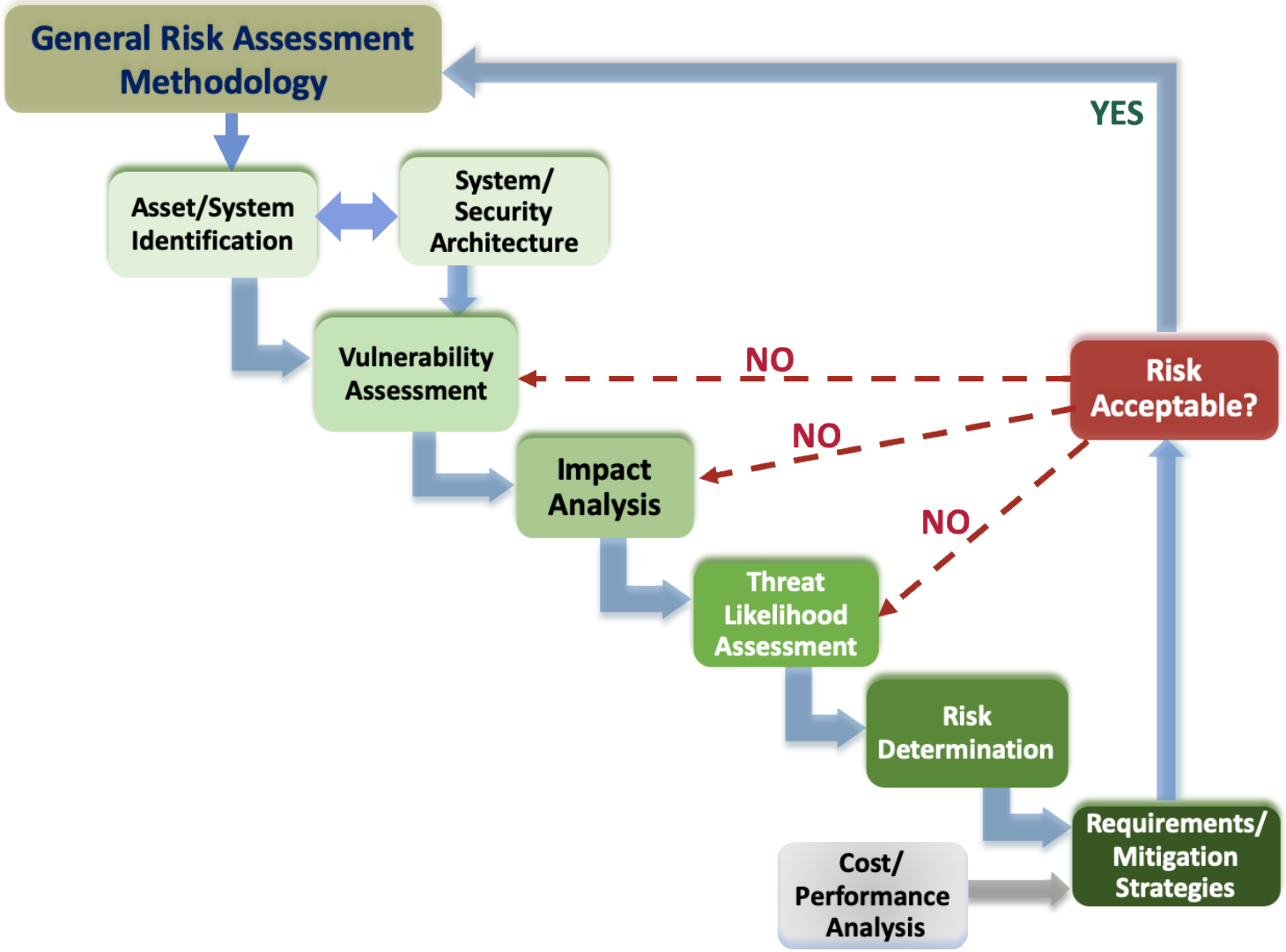

Figure 5: General Risk Assessment Methodology

The next two figures illustrate the risk assessment process during the system implementation and operations phases. The components are the same in both figures, with minor variations in the process. Either process may be used.

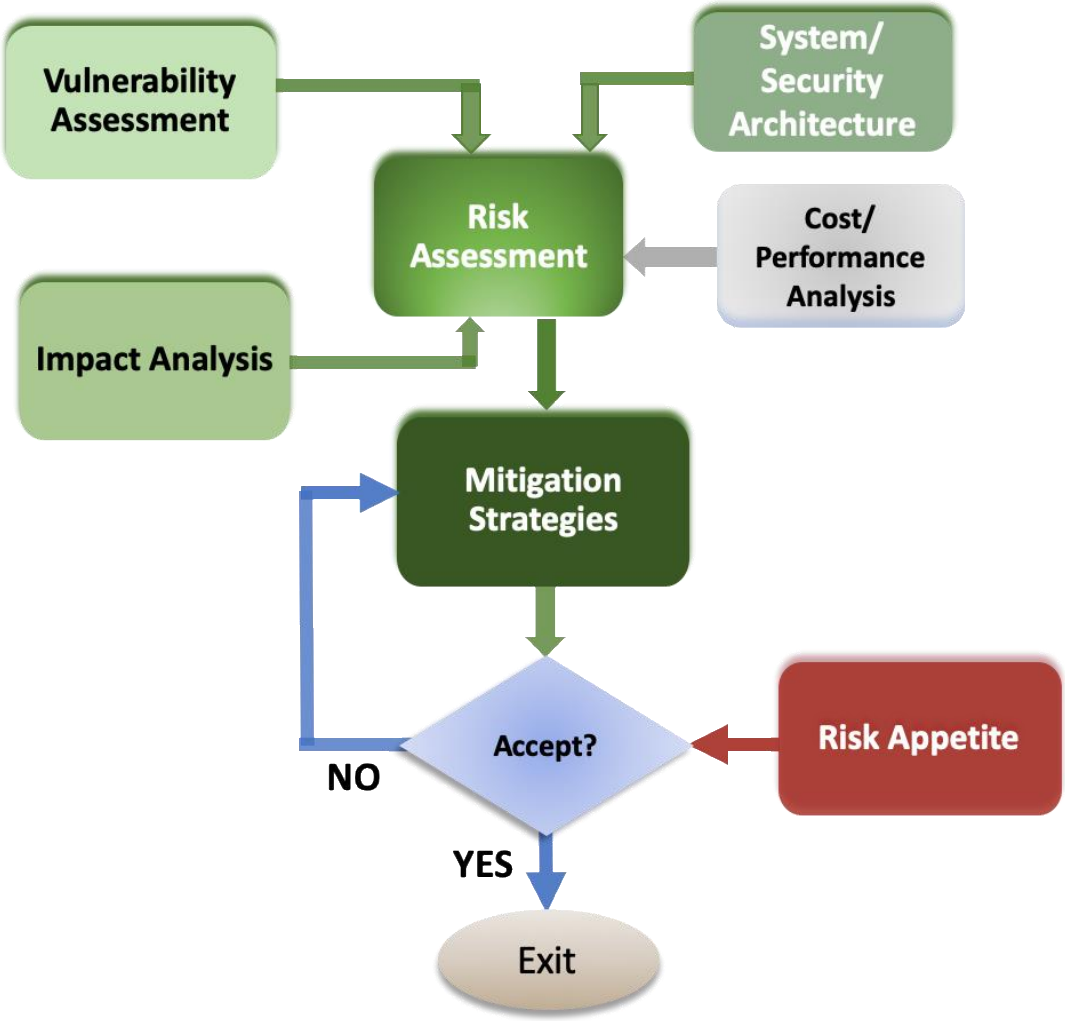

Figure 6: Implementation and Operations Phases Risk Assessment Process

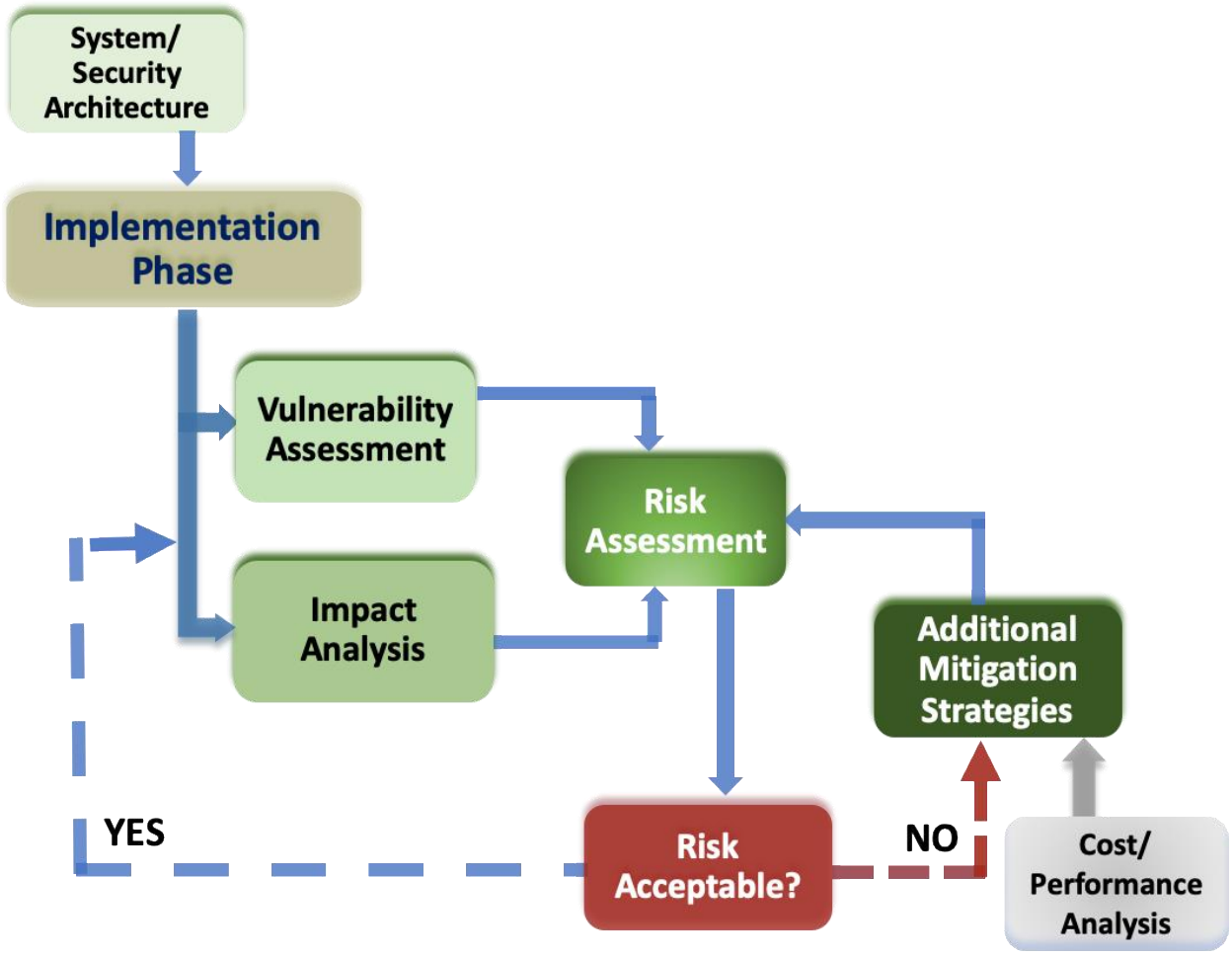

Figure 7: Implementation and Operations Phases Risk Assessment Process

The definitions of the risk assessment components are included below:

- *Asset/System Identification*: The first step in the general risk assessment process is to identify the assets and systems. This should include IT and OT hardware, software/firmware, data, and documentation that support the functions, both critical and non-critical. The utility should develop criteria to define a system, basing the definition on common business functions. This should include a determination of criticality and analysis of dependencies and interdependencies.

- *System/Security Architecture*: A physical security architecture includes the components/devices, access points, and interfaces. A logical security architecture typically is an overlay on the physical security architecture and includes the communication protocols and mitigation strategies (if implemented). These architectures may be developed using the utility's system architecture.

    - An important use of the security architecture is to identify the *attack surface* and the *attack vectors*. The attack surface describes all of the different points where an attacker could get into a system, for example through the network, software, or humans. An attacker uses a system's resources to attack a system, therefore, a

system's resources contribute to the system's attack surface. The more exposed the system's surface, the more attack opportunities, and the more likely it will be a target of attack. The attack vector defines the specific method or path that an attacker uses when exploiting a vulnerability. Attackers often use social engineering techniques, such as phishing, to acquire access. As the Internet of Things (IoT), Industrial Internet of Things (IIoT) and other new technologies proliferate, the attack surface and the number of attack vectors increase.

- *Vulnerability Assessment*: A cyber component is vulnerable if physical, procedural, documentation, or weaknesses exist that allow a threat actor to adversely affect the cyber component. Vulnerabilities include:
    - Misconfigurations
    - Software bugs
    - Lack of physical access controls and physical security
    - Lack of configuration management
    - Incompatible hardware that impacts firmware

  Included in the vulnerability assessment is a determination of the threat agent(s) that may exploit the vulnerability.

- *Impact Analysis*: this includes the *impact* and the *likelihood/opportunity*. Impact is the effect of an event, incident, or occurrence. This includes determining the level and type of damage or loss that can occur and may include loss of life, brownouts or blackouts, and/or loss of public confidence. *Likelihood/opportunity* is a measure of how easily and effectively an attacker can exploit a vulnerability to achieve a malicious effect. Some of the criteria are listed below. (Note: the full set of impact and likelihood/opportunity criteria are included in Section **Error! Reference source not found.**):
  Component's attack surface
    - Component's attack surface
    - Direct or indirect physical/logical access
    - Competence/knowledge of the attacker
    - Trust level implemented in the system
    - Reconnaissance time for the attacker that has access to the system
    - Types of vulnerabilities present
    - Availability of attack tools. These may be publicly available or require special knowledge
    - Cost to exploit

- *Risk Assessment Determination*: Included in the determination are the impact and the likelihood/opportunity. The risk decision is one of the following: mitigate, accept, transfer, or avoid. Utilities are typically conservative in their risk posture, particularly for the OT systems because of the potential for loss of life.

- *Security Requirements/Mitigation Strategies:* These include policies, procedures, technologies, and tactics to reduce/minimize the risk.

- *Cost/Performance Analysis*: Prior to implementing a mitigation strategy the utility considers the cost and potential performance impact. If the cost is excessive, the performance is negatively impacted, and/or the control conflicts with other security controls, the utility may consider implementing a compensating control. A compensating

control is an alternative control to meet the security requirement. Because of latency issues with OT devices, impact on performance is an important consideration.

- In the operations and implementation phases, *continuous monitoring* is performed to ensure that the security controls continue to be effective. Also, with the deployment of new devices, the upgrade of existing devices, or the identification of new attack vectors, the risk may have changed.

- *Other Factors*: there are two additional factors that are relevant to the energy sector:

    - *Criticality*: the value of the cyber component as it relates to the cyber application or system. A cyber component is critical when its compromise has a significant effect on system operations. Criticality may change over time. This applies within a company and across companies.

    - *Interdependencies:* identification of the interdependencies between the energy sector and other sectors. This may be used in determining potential cascading impacts 2ithin the energy sector, e.g., generation, transmission, distribution and with other sectors such as water, finance, etc.

2.1 Threat Agents

Vulnerabilities are exploited by different threat actors. While there are many threat actors out there today, most of them fit into the following categories.

Government/State Sponsored: These groups are well funded and often build sophisticated, targeted attacks. They are typically motivated by political, economic, technical, or military agendas. They are often looking for competitive information, resources or users that can be exploited for espionage purposes. They can execute large-scale attacks and advanced persistent threat (APT) attacks.

Organized Crime: Most often, these cybercriminals engage in targeted attacks driven by profits. They are typically either looking for personally identifiable information (PII) of customers or employees, such as social security numbers, health records, credit cards, and banking information, or to hijack and ransom critical digital resources.

Hacktivists: These attackers have a political agenda. Their goal is to either create high-profile attacks that help them distribute propaganda, or to cause damage to organizations they oppose. The ultimate goal is to find a way to benefit their cause or gain awareness for their issue. Hacktivists want to undermine your reputation or destabilize your operations. Vandalism is their preferred means of attack.

Insider Threat: Attackers operating inside the organization are typically disgruntled employees or ex-employees either looking for revenge or some type of financial gain. They may collaborate with other threat actors, such as organized crime or government sponsored hackers.

Opportunistic: These attackers are usually amateur criminals, often referred to as script kiddies, who are driven by the desire for notoriety. Sometimes they find and expose flaws and exploits in network systems and devices.

Internal User Error: Users making mistakes with configurations are typically the largest threat organizations face. These threat actors exist largely due to failing to design flaws out of the network or system, or by providing privileges to individuals who should not have them. Internal user errors have been known to bring down critical resources such as firewalls, routers, and servers.

2.2 Risk Assessment Computation

There are two methods to determine risk, qualitative and quantitative. Quantitative risk assessment uses mathematical formulas to determine risk. Qualitative risk assessments typically organize risk into low, medium, and high.

The classic quantitative risk formula is: risk = impact x probability[6]. In the current environment, the potential impact constantly increases because of the increasing dependence on digital technology. Probability is a function of threat and vulnerabilities and includes likelihood and opportunity. As with impact, both threats and vulnerabilities are increasing. For example, there are attack tools that are freely available and with the increased interconnectivity of systems and the installation of digital devices, the vulnerabilities have increased. Consequently, the level of cyber security risk over time will increase. The following diagram illustrates this increased risk. (Note: the specific curve requires detailed data.)

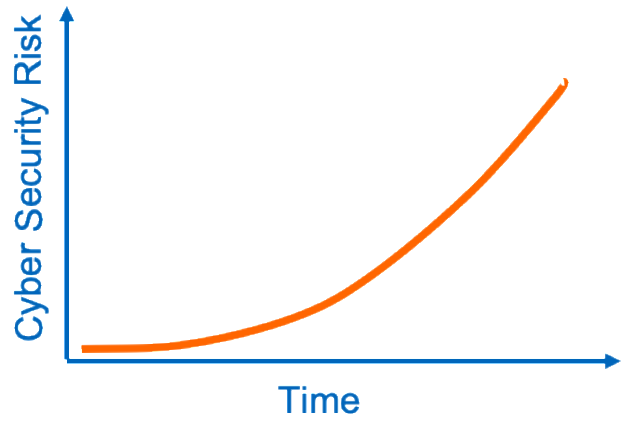

Figure 8: Risk over Time Curves

The role of cyber security is to *reduce* risk, particularly as the level of cyber security capabilities increase. The risk reduction formula is: $\text{Risk} = \frac{\text{Impact x Likelihood/Opportunity}}{\text{Cyber Security Capabilities}}$

The following curve illustrates a *reduction* in risk as cyber security capabilities increase.

[6] The remaining content in this section is extracted from a briefing presented by Jason Christopher, Chief Technology Officer, Axio Global, Inc. at the November 2019 UCSI meetings. Jason is currently the Principal Cyber Risk Advisor, Dragos, Inc.

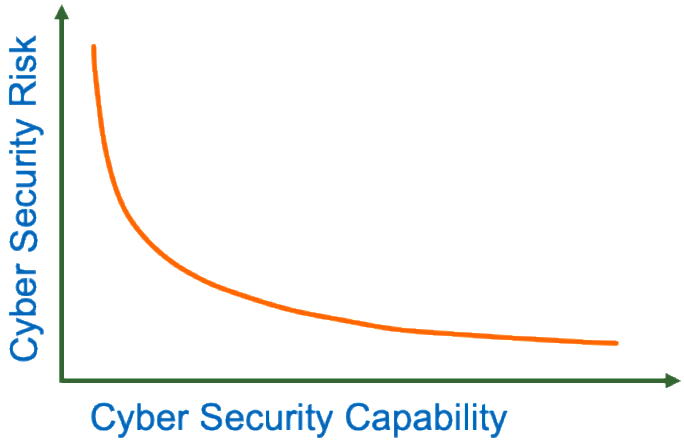

Figure 9: Risk Reduction Curve

As with the previous figure, the exact curve will depend on specific data.

2.3 Risk Ranking

For all risk assessment approaches, the two inputs are probability (likelihood and opportunity), and impact. In the National Electric Sector Cybersecurity Organization Resource (NESCOR) project, a quantitative methodology was developed. The methodology includes two components in the ranking process: impact and effects on likelihood and opportunity. Following is the process for performing a risk assessment using the NESCOR method.

2.3.1 Risk Assessment Steps

The steps in the risk assessment process are as follows:

1. Develop an initial list of the utility's high priority systems. Typically, these are large substations.

2. Select one or more of these high priority systems for the initial risk assessments.

3. Select and tailor one or more NESCOR failure scenarios that are applicable to each system. The tailoring is to ensure that the scenario accurately represents the deployed configuration.

4. Review the Impact and Likelihood and Opportunity criteria for applicability. The criteria are general and intended for use by all utilities that have generation, transmission, and/or distribution functions. The criteria that will need the most tailoring are the Impact Criteria. For example, the *GDPR Data Protection Violation* and *Negative impact on billing functions* may not be applicable for generation utilities. The utility can either remove these criteria, mark them as N/A (not applicable), or score them as zero. It is important to use the same set of criteria for all systems in the utility to ensure consistency. Some criteria may need to be revised for the utility. For example, most utilities have specific regularity requirements for ensuring the reliability/availability of electricity. The specific Impact criteria is "Negative impact on customer service." This

criterion should be revised to include the regulatory language. Included in Appendix B are regulations for Georgia and Ukraine.

5. Score each failure scenario using the impact and likelihood criteria (each line item in Table 1 and Table 2, respectively).

6. Combine the scores for the set of impact criteria, to create a single numerical composite impact score. Likewise, combine the scores for the set of likelihood criteria, to create an overall likelihood score.

7. The final step is done after ranking results for the initial set of systems have been compiled. The results of Step 7 can be displayed graphically as shown in Figure 10 below. The highest ranking risks are located in the upper right quadrant – with high impact and high likelihood and opportunity scores. The systems that are included in the upper right quadrant are of the highest priority in relation to risk.

8. Develop a baseline profile for the utility. For the UCSI members, this would involve conducting a C2M2 assessment for the transmission or distribution function. This will be used by the utility to identify the system gaps and vulnerabilities.

9. The final step is to identify the associated mitigation strategies that are the most effective. These mitigation strategies need to be evaluated based on cost and potential performance impacts.

2.3.2 Impact Criteria

Table 1 shows the impact criteria. Impact is the effect of the failure scenario on the delivery of power, the business of the utility, and the interests of its customers.

- **System Scale:** Describes whether the impact of this failure scenario is geographically localized or may impact the entire system.

- **External Customers**: This criterion considers whether external customers, such as other utilities, are impacted.

- **Safety Concern:** Two safety criteria consider whether there is a potential for injuries or loss of life. This factor is considered for the public and the utility workforce.

- **Ecological Concern:** This criterion considers whether the failure scenario might cause damage to the environment. For example, burning or leaking of hazardous material would be judged as “Permanent Ecological Damage.”

- **Financial Impact of Compromise on Utility:** This criterion considers direct financial loss to the utility as a result of the failure scenario, without consideration of the restoration costs as defined below. A scale for costs is used that is relative to the amount of utility revenue.

- **Restoration Costs:** Restoration costs include the cost to return the system to proper operation, not including any legal or other reparations as a result of the failure. A scale for costs is used that is relative to the total size of the utility operations and maintenance

budget.

- **Negative impact on generation:** The scoring for this criterion considers the level of loss of generation, and for how long this loss is sustained.

- **Negative impact on the energy market:** Specific impacts identified are price manipulation, lost transactions, or loss of participation by market members (buyers or sellers). Scores 0, 1 and 3 mean respectively either no such impacts, local impacts or widespread occurrence of these impacts. A breakdown in key market functions that creates a non-operational market earns the highest score.

- **Negative impact on the bulk transmission system:** A *major transmission system interruption* is defined as follows: “An event has occurred that required action(s) to relieve voltage or loading conditions; or transmission separation or islanding has occurred.” A *complete operational failure or shut-down of the transmission* system is defined as: “An emergency event where an electrically isolated or interconnected electrical system suffers total system collapse that results in the shutdown of the transmission …electrical system….”

- **Negative impact on customer service:** The scores for this criterion consider the delay a customer experiences in gaining resolution of their problem, and for how long this condition persists. The example failure scenario could cause disruption to customer service due to increased call volume for more than a week if the meter issue becomes public knowledge.

- **Negative impact on billing functions:** Billing depends upon accurate power usage data. This criterion measures the number of customers for which the utility may lose the capability to generate accurate bills due to the failure scenario. The scores also consider whether or not the data is recoverable.

- **Destroys goodwill toward utility:** This criterion measures the extent to which customers and the community look less favorably on the utility as a result of the occurrence of the failure scenario. It is scaled by the resulting level of decrease in interest by customers in participating in advanced programs such as smart meter deployments and demand response.

- **Immediate economic damage, Long term economic damage:** Economic damage means a negative impact on the wealth and resources of a country or region. (This is distinct from a financial impact on an organization or individual.) The scoring for these criteria is based upon how widespread the damage is, and for how long it continues to have impact.

- **Causes a loss of privacy for a significant number of stakeholders:** The scale for this criterion considers the number of customers who may have personal information disclosed due to the failure scenario.

- **General Data Protection Regulation (GDPR) Data Protection Violation:** Each supervisory authority shall have the corrective powers specified in Appendix A.

- **Legal liability:** This criterion considers the legal liability for non-malicious and malicious cyber security events that may result in lost revenue, power brownouts or blackouts, exfiltration of personal information, or injury and/or death. the examples: lost revenue from a network interruption arising from ransomware, network shutdown at a critical third-party vendor reduces or completely stops operations, hackers enter the network and turn off safety measures, leading to massive pollution, exfiltration of personal health and financial records, modification of the power system controls resulting in injury and/or death.

- **The Directive on Security of Network and Information Systems (NIS Directive) Non-compliance:** The responsibility to determine penalties for non-compliance lies with the individual Member States and not the EU. The Directive states that penalties must be "effective, proportionate, and dissuasive." Organizations that fail to comply with the NIS Directive are subject to reactive ex-post supervisory activities by National Competent Authorities (NCAs). (The non-compliance penalties are included in Appendix A.)

Table 1: Impact Scores

Criterion	How to score
System scale	0: single utility customer, 1: small geographic area, 3: town or city, 9: potentially full utility service area and beyond
External customers, e.g., other utilities	0: none, 1: high voltage customer, 3: DSO, generation capacity, 9: transnational interconnections, ENTSO-E interconnected systems
Public safety concern	0: none, 1:1-20 injuries possible, 3: 100 injured possible, 9: one death possible
Workforce safety concern	0: none, 3: any possible injury, 9: any possible death
Ecological concern	0: none, 1: local ecological damage such as localized fire or spill, repairable, 3: permanent local ecological damage, 9: widespread temporary or permanent damage to one or more ecosystems such as the Exxon Valdez or Chernobyl
Financial impact of compromise on utility	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%
Restoration costs - cost to return to normal operations, not including any ancillary costs	0: Petty cash or less, 1: < 1% of utility organization O&M budget, 3: <=10%, 9: > 10%
Negative impact on generation	0: No effect, 1: Small generation facility off-line or degraded operation of large facility, 3: More than 10% loss of generation for 8 hours or less, 9: More than 10% loss of generation for more than 8 hours
Negative impact on the energy market	0: No effect, 1: localized price manipulation, lost transactions, loss of market participation 3: price manipulation, lost transactions, loss of market participation impacting a large metro area, 9: market or key aspects of market non-operational

Criterion	How to score
Negative impact on the bulk transmission system	0: No effect, 1: loss of transmission capability to meet peak demand or isolate problem areas, 3: Major transmission system interruption, 9: Complete operational failure or shut-down of the transmission system
Negative impact on customer service	0: No effect, 1: up to 4 hour delay in customer ability to contact utility, and gain resolution, lasting one day, 3: up to 4 hr. delay in customer ability to contact utility and gain resolution, lasting a week, 9: more than 4 hr. delay in customer ability to contact utility and gain resolution, lasting more than a week
Negative impact on billing functions	0: None, 1: isolated recoverable errors in customer bills, 3: widespread but correctible errors in bills, 9: widespread loss of accurate power usage data, unrecoverable
Destroys goodwill toward utility	0: No effect, 1: negative publicity but this doesn't cause financial loss to utility, 3: negative publicity causing up to 20% less interest in advanced programs, 9: negative publicity causing more than 20% less interest in advanced programs; loss of major accounts
Immediate economic damage - refers to functioning of society as a whole	0: none, 1: local businesses down for a week, 3: regional infrastructure damage, 9: widespread runs on banks
Long term economic damage	0: none, 1: (not used), 3: several year local recession, 9: several year national recession
Causes a loss of privacy for a significant number of stakeholders	0: none, 1: 1000 or less individuals, 3: 1000's of individuals, 9: millions of individuals
GDPR Data Protection Violation	0: no violation, 1: minor violation, 3: clear violation, 9: significant violation
Legal Liability	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%
NIS Directive Non-Compliance	0: no violation, 1: minor violation, 3: clear violation, 9: significant violation
Total – impact	**Maximum possible score: 171**

2.3.3 Likelihood and Opportunity Criteria

Table 2 lists criteria that influence the likelihood and opportunity for a threat agent to exploit a failure scenario. A utility can use these criteria to help assess the probability that a cyber security incident will occur. The criteria do not include specific probabilities, because such a prediction is speculative as well as dependent upon a number of factors for a specific utility. For example, a terrorist organization would be more interested in attacking a "high profile" organization than one that is relatively unknown outside its customer base.

For these criteria, scores get higher as the “cost” to the threat agent gets lower and therefore as the likelihood and opportunity increases.

- **Skill Required:** This criterion rates the skill and specialized knowledge that it takes for a threat agent to cause the failure scenario to occur.

- **Accessibility (Physical):** This criterion scores the difficulty of obtaining physical access that is required to cause a failure scenario. Accessibility ranges from easy and obvious to obtain for anyone, to not feasible to obtain.

- **Accessibility (Logical):** This criterion in similar to the previous one. Logical access refers to any non-physical form of access required to cause a failure scenario, such as network access or a particular utility employee’s phone number. The scoring of this criterion assumes that physical access has already been achieved.

- **Attack Vector – ease of exploit:** This criterion evaluates how easy it is to obtain the technical means to carry out a failure scenario, once physical and logical access have been achieved. The exploit may be simple to carry out with little further effort given physical and logical access. There may be tools available for download from the Internet, or available instructions for the exploit or for similar exploits, or the exploit may be theoretical at this time.

- **Attack vector – ease of discovery by threat agents**: This criterion scores how easy it is for the threat agents to discover the vulnerability. Ease of discovery ranges from practically impossible to publicly available with automated tools available.

- **Attack vector – awareness by threat agents**: This criterion specifies how well known this vulnerability is to threat agents. Awareness ranges from unknown to publicly available.

- **Occurrence of vulnerability:** This criterion scores how extensively the vulnerability is deployed throughout the electric sector. This includes both the IT and OT systems within a utility that are used to support the power system operations. A vulnerability that is shared among many organizations and in many contexts is more likely to be exploited. Occurrence ranges from isolated deployment to nearly all utilities.

- **Motivation:** This criterion specifies how motivated the threat agents are to find and exploit the vulnerability. Motivation ranges from no reward to high reward.

- **Size/coordination of threat agents**: This criterion identifies the size of the group of threat agents. Size ranges from a single individual to a nation state/criminal organization.

Table 2: Likelihood and Opportunity Scores

Criterion	How to score
Skill required	0: Deep domain/insider knowledge and ability to build custom attack tools, 1: Domain knowledge and access to cyber attack techniques, 3: Special insider knowledge needed, 9: Basic domain understanding and computer skills
Accessibility (physical)	0: Inaccessible, 1: Guarded, monitored, 3: Fence, standard locks, 9: Publicly accessible
Accessibility (logical, assume have physical access)	0: High expertise to gain access, 1: Not readily accessible, 3: Publicly accessible but not common knowledge, 9: Common knowledge or none needed
Attack vector - ease of exploit (assume have physical and logical access)	0: Theoretical, 1: Similar attack has been described, 3: Similar attack has occurred, 9: Straightforward, script or tools available
Attack vector – ease of discovery by threat agents	0: Extremely difficult, 1: Difficult, 3: Easy, 9: Publicly known
Attack vector – awareness by threat agents	0: Unknown, 1: Hidden/difficult to find, 3: Obvious, 9: Publicly known
Occurrence of vulnerability	0: Isolated occurrence, 1: More than one utility, 3: Half or more of power infrastructure, 9: Nearly all utilities
Motivation	0: No reward, 1: Possible reward, 3: Low reward, 9: High reward
Size/coordination of threat agents	0: Nation state/criminal organization, 1: Developers, partners, administrators, 3: Compromised internal account/user, 9: Local access by Internet user
Total – likelihood and opportunity	**Maximum possible score: 81**

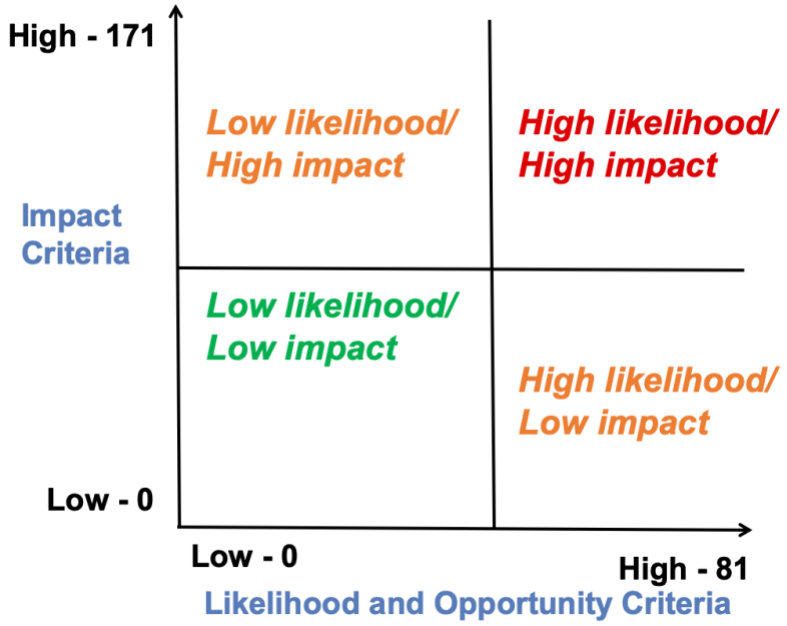

Figure 10: Risk Ranking

Included in Appendix B is an example of scoring a failure scenario.

2.4 Mitigation Strategies

Risk mitigation includes the selected tactics, techniques, and procedures. However, prior to implementing a specific mitigation strategy, the utility assesses the potential cost and performance impact. Also, the strategy is assessed against currently deployed strategies, to ensure there is no conflict.

2.5 Risk Assessment Methodology Tips[7]

The following tips may be used to guide the risk assessment.

1. A cyber security risk assessment should be performed at several stages throughout a system life cycle. For example, an initial assessment is used as input for developing cyber security requirements in the design phase. This assessment will not be at a detailed level. In this initial cyber security risk assessment:
    a. Identify *all* systems and assets, not just the critical cyber assets
    b. Specify preliminary confidentiality, integrity, and availability impact levels for each system based on system criticality and identification of threats and vulnerabilities.
    c. A high in one security objective for a system does NOT mean that the overall impact level for the system must be high. Because the impact levels may not be the same, this will require additional analysis to address these differences.

[7] This section was extracted from *Cyber Security Strategy Guidance for the Electric Sector*, EPRI, Palo Alto, CA: 2012. 1025672, and revised.

2. A risk assessment should be conducted throughout a system life cycle. After the design phase, a risk assessment should be performed at regular intervals, e.g., yearly; when there are major technology changes; and when the threat environment, including the attack surface, increases.

3. Because the focus in the initial risk assessment is on developing security requirements, vulnerability identification will typically be at a high level corresponding to classes of devices/components.

4. There are two basic types of risk assessment – *qualitative* where the scoring may be low, moderate, and high and *quantitative* where the scoring may be 1-10. A utility should select the approach they believe will provide the most useful results.

3 CURRENT THREAT ENVIRONMENT

Some of the documented trends are based on general analysis of cyber security. For the trends based on interviews or assessments related to cyber security incidents, the majority of organizations were outside the energy sector. However, since cyber security is relevant to all sectors, and with the increasing interconnection of systems, these should be considered.

3.1 2019 Security Trends

According to Ponemon[8], the highest-rated cybersecurity concerns for 2019 are third-party risks, data breaches and attacks on IoT or Operational Technology (OT) assets. Forty-eight percent of respondents say their organization experienced a significant disruption to business processes caused by malware and 41 percent of respondents say a third party misused or shared confidential information with other third parties. Both of these security incidents are expected to increase in frequency in 2019.

According to CrowdStrike[9], "Malware continues to loom as a primary feature of the threat landscape, but it is often only the precursor to an attack, not the ultimate objective. Initial intrusion leads to more sophisticated and stealthy techniques, such as "living off the land" tradecraft that uses legitimate tools already present on the target system to accomplish adversary objectives." During earlier phases of operation threat agents increasingly use this methodology, leveraging native system commands, applications, and software to gain access to the system and move throughout the network undetected.

Another technique documented by CrowdStrike and other organizations is *malware-free* attacks. This involves "fileless" exploits, where no executable file is written to disk. These attacks are particularly effective at evading traditional antivirus solutions, which look for files saved to disk so they can scan them and determine if they are malicious. Exploits and exploit kits commonly are used to execute attacks directly in memory by exploiting vulnerabilities that exist in the operating system or in installed applications and stolen credentials are leveraged for remote logins using known tools. Attackers can establish persistence without writing anything to disk by hiding code in the registry, the kernel, or by creating user accounts that grant them at-will access to systems.

Finally, as sophisticated attacks continue to evolve, enterprises face much more than just "a malware problem." Defenders must look for early warning signs that an attack may be underway, such as code execution, persistence, stealth, command control and lateral movement within a network. Contextual and behavioral analysis, when delivered in real time via machine learning and artificial intelligence, effectively detects and prevents attacks that conventional "defense-in-depth" technologies cannot address.

Dragos has focused their assessments and analysis on ICS. They identified the following trends for 2018.

---

[8] *Measuring & Managing the Cyber Risks to Business Operations*, sponsored by Tenable, Independently conducted by Ponemon Institute LLC, Publication Date: December 2018

[9] CrowdStrike, 2019 *Global Threat Report, Adversary Tradecraft and the Importance of Speed*.

- *From the ICS Activity Groups and Threat Landscape report*[10]: Third-party access to OT networks is a common and necessary component of modern operations. However, the OT network access granted to vendors and others can also expose an asset operator to significant risk as compromises can move from vendors' networks to the asset operator's network. Third-party or supply chain compromise leverages explicit trust between parties and bypasses a large part of the security stack, potentially including perimeter defenses, such as firewalls or proxy servers, to access a target. Once an adversary accesses the victim network, it is possible to pivot throughout the network, steal credentials or other sensitive data, and further embed themselves within IT or operations.

- *From the Industrial Control System Vulnerability report*[11]: Patching disparity continues to be an issue. Patching, especially patching field devices or industrial network equipment, can be challenging for most operators to perform in a timely manner. Even when patched, most programmable logic controllers (PLCs) use insecure-by-design configuration protocols, making actual exploitation of these systems moot. Protocol translators such as serial to Ethernet converters are much the same – even without the ability to reconfigure the device, an attacker can take advantage of the insecure-by-design serial protocol using only the exposed features of such a translator, issuing commands to the serial device without authentication in most cases.

  While an attacker may try to take advantage of a protocol translator vulnerability, many of these systems allow unauthenticated configuration changes at a minimum. These configuration changes, both for field devices and for protocol translators, provide an easy avenue for at least denial-of-service – the attacker can easily change a system IP address and deny the owner's ability to communicate.

Crowd Research conducted an assessment of insider threat[12]. Although the assessment was not limited to the electric sector and OT devices, the results are useful for all utilities.

1. Ninety percent of organizations feel vulnerable to insider attacks. The main enabling risk factors include too many users with excessive access privileges (37%), an increasing number of devices with access to sensitive data (36%), and the increasing complexity of information technology (35%).

2. A majority of 53% confirmed insider attacks against their organization in the previous 12 months (typically less than five attacks). Twenty-seven percent of organizations say insider attacks have become more frequent.

3. Organizations are shifting their focus on detection of insider threats (64%), followed by deterrence methods (58%) and analysis and post breach forensics (49%). The use of user behavior monitoring is accelerating; 94% of organizations deploy some method of

[10] Dragos, *Year in Review 2018, ICS Activity Groups and the Threat Landscape.*

[11] Dragos, *Year in Review 2018, Industrial Control System Vulnerabilities.*

[12] Crowd Research, *Insider Threat, 2018 Report.*

monitoring users and 93% monitor access to sensitive data.

4. The most popular technologies to deter insider threats are Data Loss Prevention (DLP), encryption, and identity and access management solutions. To better detect active insider threats, companies deploy Intrusion Detection and Prevention (IDS), log management and security incident and event management (SIEM) platforms.

5. The vast majority (86%) of organizations already have or are building an insider threat program. Thirty-six percent have a formal program in place to respond to insider attacks, while 50% are focused on developing their program.

3.2 Advanced Persistent Threats (APT)

The following information is extracted from the Mandiant report: Mandiant/FireEye Report *M-TRENDS*, 2019 and identifies the primary threat actors that execute APTs. The conclusions are based on work performed in 2018 and forecasted for 2019. Although the energy sector was included and was only 4% of the industries investigated, the assessment of the respective APTs is useful.

In 2018, North Korea, Russia, China and Iran posed the greatest global cyber espionage threats worldwide. Motivated by security and economic concerns, North Korean operators matured in both technical and operational sophistication. Russian cyber espionage actors have continued to operate worldwide, targeting political entities relevant to Russia's strategic national interests. Dormant Chinese espionage teams returned and reinvented their operations, as observed during the course of Mandiant incident response engagements. Iran-nexus intrusion activity demonstrated an expanded use of cyber espionage operations to collect strategic information on national security, economics and the internal security of their targets. Finally, open source tools are now used across most major APT operators, which increases the challenge of definitive attribution.

4 CYBER SECURITY RECOMMENDATIONS

Included in this section are recommendations for utilities to mitigate potential cyber security vulnerabilities and attacks. Because the threat environment is constantly changing, the recommendations are extracted from recent reports.

4.1 Dragos Recommended Strategies

Dragos[13] recommends for an ICS environment to be considered defensible, organizations must:

1. Develop a defense-in-depth strategy that enables the safety of the facility. Preventative controls should limit access to the facility without hampering the resilience or operation of the facility.

2. Have visibility and situational awareness beyond monitoring network traffic or keeping an asset inventory. Adding ICS security-centric knowledge to ongoing communications and assets facilitates an understanding of their roles and their importance to the overall industrial process.

3. Have staff and trained resources to actively monitor and understand behaviors (good and bad) occurring across facilities.

4.2 SANS Recommended Best Practices[14]

SANS developed the following recommendations, based on a survey conducted on Industrial Internet of Things (IIoT) devices:

- Lightweight, easy to implement, and included in almost all of today's IP-based products, the use of Web services to interface with devices is also popular, despite concerns and challenges from both IT and security perspectives, not to mention difficulty with enterprise wide asset management leading to risky configuration inconsistencies among devices. When using a Web-based interface to communicate with IIoT devices, be sure to identify and address potential concerns and the resulting vulnerabilities:

    - Change default passwords, watch for hard-wired passwords and strongly consider adopting password rotation mechanisms that avoid password duplication and re-use.

    - Manage IIoT assets and develop and maintain a real-time inventory that includes your connected devices. Use this inventory to keep products up to date, ensuring that all patches and updates are from approved and trusted sources.

    - Ensure that vulnerability disclosures related to the product or services employed by the product are carefully considered and, when possible, patch products or add

[13] Dragos, *Year in Review 2018, Lessons Learned from Threat Hunting & Responding to Industrial Intrusion.*
[14] SANS, *The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns*, 2018.

compensating technical and nontechnical controls to mitigate risks.

- Disable unnecessary ports and services and monitor network traffic for future indications of activity to those ports or services. This can also help guard against non-network-based vulnerabilities such as direct connections into the device.

- Test products in a highly controlled environment absent of safety risks to personnel, machinery and the environment for vulnerabilities that range from resource exhaustion and denial.

- Establish your own long-term strategy to achieve IIoT *cyber hygiene* within your organization. Pay special attention to IIoT endpoint management, especially in terms of asset inventory, asset configuration and continuous monitoring of those assets.

4.3 CrowdStrike Recommendations[15]

CrowdStrike recommends that all organizations consider the following measures to help maintain strong defenses in 2019:

4.3.1 Basic Hygiene Still Matters

The basics of user awareness, asset and vulnerability management, and secure configurations continue to serve as the foundation for a strong cybersecurity program. CrowdStrike recommends that organizations regularly review and improve their standard security controls, including the following:

- **User awareness** programs should be initiated to combat the continued threat of phishing and related social engineering techniques, such as 2018's massive Emotet outbreak.

- **Asset management** and software inventory are crucial to ensuring that organizations understand their own footprint and exposure.

- **Vulnerability** and patch management can verify that known vulnerabilities and insecure configurations are identified, prioritized and remediated.

- **Multifactor authentication (MFA)** should be established for all users because today's attackers have proven to be adept at accessing and using valid credentials, leading quickly to deeper compromise — also, MFA makes it much more difficult for adversaries to gain privileged access.

- **In addition to MFA**, a robust privilege access management process will limit the damage adversaries can do if they get in and reduce the likelihood of lateral movement.

- **Implement password** protection to prevent disabling or uninstalling endpoint protection that provides critical prevention and visibility for defenders — also, disabling it is always a high-priority for attackers looking to deepen their foothold and hide their activities.

[15] CrowdStrike, *2019 Global Threat Report – Adversary Tradecraft and the Importance of Speed,* 2019.

4.3.2 *Look Beyond Malware: Strengthen Defenses Against Modern Attacks*

As sophisticated attacks continue to evolve, enterprises face much more than just "a malware problem." Defenders must look for early warning signs that an attack may be underway, such as code execution, persistence, stealth, command control and lateral movement within a network. Contextual and behavioral analysis, when delivered in real time via machine learning and artificial intelligence, effectively detects and prevents attacks that conventional "defense-in-depth" technologies cannot address.

4.4 Center for Internet Security (CIS) Security Controls[16]

The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of IT experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors including, retail, manufacturing, healthcare, education, government, defense, and others. Although the list focuses on IT systems, the majority of the controls are also applicable to OT systems.

Figure 11: CIS Top 20 Security Controls, V7

[16] Center for Internet Security, *CIS Controls, V7,* 2018.

5 TOOLS

There are several tools and guidance documents that are publicly available and may be used as part of the risk management methodology. These tools are summarized below, with references to the associated website.

5.1 ICS Kill Chain[17]

The following diagrams and the descriptions are extracted from the SANS Report referenced in the footnote. The report includes detailed descriptions of the phases within each Stage of the attack. The document is publicly available. The material in this section provides an overview of the ICS Kill Chain.

The first stage of an ICS cyber attack is best categorized as the type of activity that would traditionally be classified as espionage or an intelligence operation. It is very similar in nature to attacks covered in Lockheed Martin's Cyber Kill Chain™ and often has the purpose of gaining access to information about the ICS, learning the system and providing mechanisms to defeat internal perimeter protections or gain access to production environments. The phases of the first stage are illustrated in Figure 12.

[17] The information on the ICS Kill Chain is extracted from the SANS Report: *The Industrial Control System Cyber Kill Chain*, Michael J. Assante and Robert M. Lee, October 2015

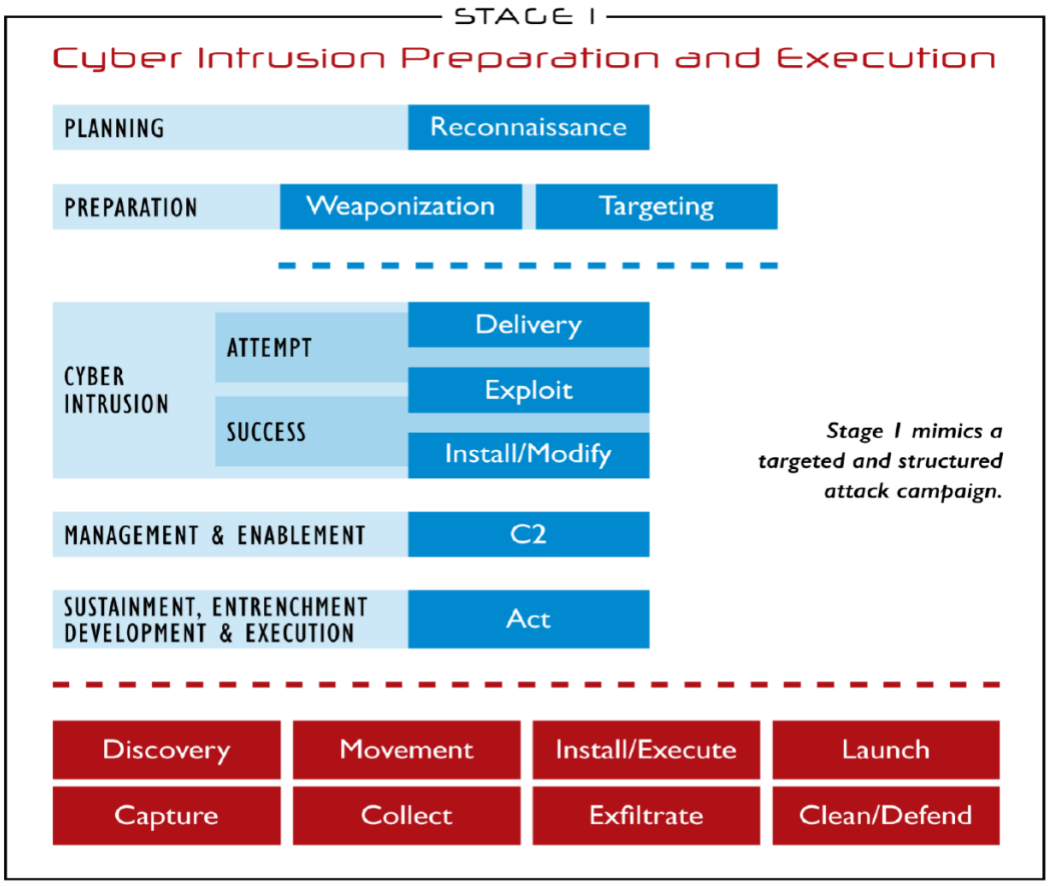

Figure 12: ICS Kill Chain: Stage 1

It is in Stage 2 that the attacker must use the knowledge gained in Stage 1 to specifically develop and test a capability that can meaningfully attack the ICS. Unfortunately, due to sensitive equipment it is possible that Stage 1 adversary operations could lead to an unintended attack. This is a significant risk for a nation-state cyber operation because such an attack may be perceived as intentional and have unforeseen consequences. For example, an attempt to actively discover hosts on an ICS network may disrupt necessary communications or cause communication cards to fail. Simple interactions with ICS applications and infrastructure elements may result in unintentional outcomes. This activity would still be contained within Stage 1 and be an unintended effect in the Act step. Intentional attacks take place in Stage 2 and are described in Figure 13.

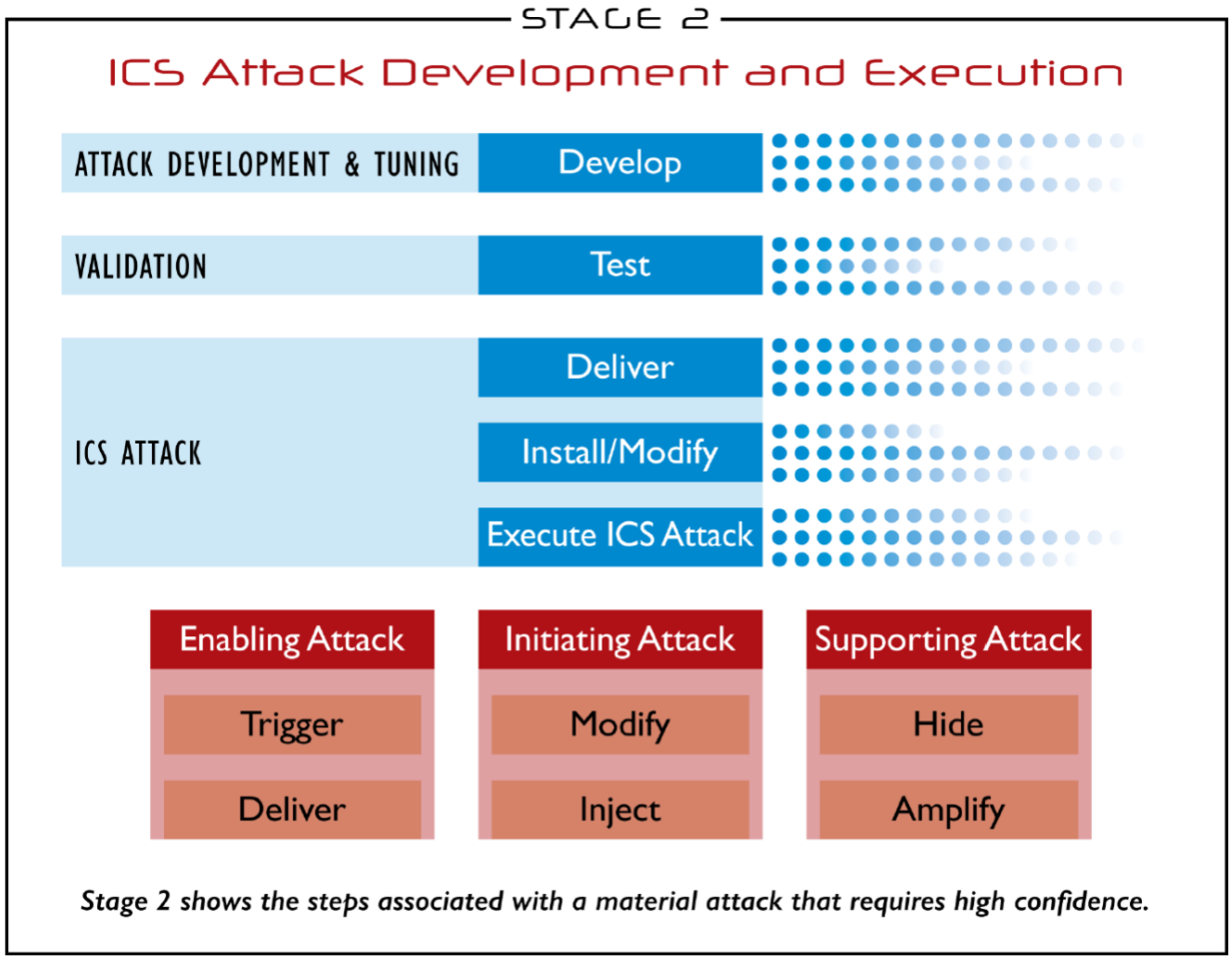

Figure 13: ICS Kill Chain: Stage 2

5.2 MITRE ATT&CK™[18] Tool

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK stand for: Adversarial Tactics, Techniques and Common Knowledge. The ATT&CK™ Model (Adversarial Tactics, Techniques, and Common Knowledge) serves as a method for discovering coverage and defense gaps inside a target network. ATT&CK is available at https://attack.mitre.org and focuses on an adversary's post-compromise behavior using the ATT&CK threat model. The purpose of ATT&CK is to provide a model for cyber adversary behavior, reflecting various phases of an adversary's lifecycle and the platforms they are known to target. The goal was to break down and classify attacks in a consistent and clear manner that can make it easier to compare and contrast them to find how the attacker exploited networks and endpoints and penetrated networks. ATT&CK may be used for:

- Threat modeling
- Red-team/blue-team planning

[18] https://attack.mitre.org/;
STIX 2 representations of ATT&CK knowledge base: https://github.com/mitre/cti

- Enhancing threat intelligence
- Defensive planning.

The ATT&CK model takes the three post-compromise stages of the cyber-attack lifecycle and expands them into 10 distinct tactics that are employed by advanced persistent threats (APTs). This is illustrated in Figure 14 below.

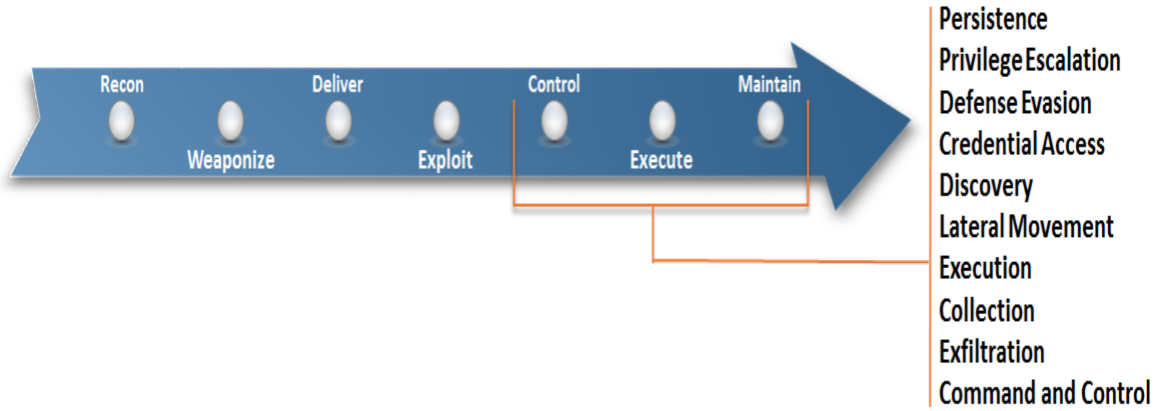

Figure 14: MITRE ATT&CK Model

The threat-based approach to network compromise detection uses a behavioral methodology and is guided by five principles that describe critical tenets of an effective threat-based approach to network security.

Principle 1: Include Post-Compromise Detection – Over time, previously effective perimeter and preventive defenses may fail to keep persistent threats out of a network. Post-compromise detection capabilities are necessary for when a threat bypasses established defenses or uses new means to enter a network.

Principle 2: Focus on Behavior – Signatures and indicators are useful with a priori knowledge of adversary infrastructure and tool artifacts, but defensive tools that rely on known signatures may become unreliable when signatures become stale in relation to a changing threat. Sophisticated defenses should also incorporate detecting and learning from post-compromise adversary behavior.

Principle 3: Use a Threat-based Model – An accurate and well-scoped threat model is necessary to ensure that detection activities are effective against realistic and relevant adversary behaviors.

Principle 4: Iterate by Design – The adversarial tool and technique landscape is constantly evolving. A successful approach to security requires constant, iterative evolution and refinement of security models, techniques, and tools to account for changing adversary behavior and to understand how networks are compromised by an Advanced Persistent Threat (APT).

Principle 5: Develop and Test in a Realistic Environment – Analytic development and refinement should be performed in a production network environment, or one that matches realistic network conditions as closely as possible. Behavior generated by real network users should be present to account for the expected level of sensor noise generated by standard network use. Whenever possible, detection capabilities should be tested by emulation of

adversary behavior within that environment.

In keeping with Principles 1 and 2, the threat model encapsulated in ATT&CK describes post-compromise adversary behaviors within enterprise networks.

5.2.1 ATT&CK Tactics and Techniques

ATT&CK is broken down into high-level adversary tactic categories and individual techniques that adversaries may use within each of the tactic categories. *Tactics* describe why an adversary performs an action, and techniques describe how they do it. *Techniques* are described in the ATT&CK model from both the offensive and defensive points of view so they are a useful reference and pivot between both disciplines. ATT&CK techniques also contain references to known examples of the technique having been used and links to public threat reporting on adversary groups known to use that technique or related tools to provide examples of adversary behavior in the wild.

Tactics represent the highest level of abstraction within the ATT&CK model. They are the tactical goals an adversary has during an operation. The ATT&CK tactic categories are:

- Persistence – Any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures.

- Privilege Escalation – The result of techniques that cause an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout a remote operation.

- Defense Evasion – Techniques an adversary may use for the purpose of evading detection or avoiding other defenses.

- Credential Access – Techniques resulting in the access of, or control over, system, domain, or service credentials that are used within an enterprise environment.

- Discovery – Techniques that allow an adversary to gain knowledge about a system and its internal network.

- Lateral Movement – Techniques that enable an adversary to access and control remote systems on a network. Often the next step for lateral movement is remote execution of tools introduced by an adversary.

- Execution – Techniques that result in execution of adversary-controlled code on a local or remote system.

- Collection – Techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration.

- Exfiltration – Techniques and attributes that result or aid in an adversary removing files and information from a target network. This category also covers locations on a system or network where an adversary may look for

information to exfiltrate.

- Command and Control – Techniques and attributes of how adversaries communicate with systems under their control within a target network. Examples include using legitimate protocols such as HTTP to carry command and control information.

5.3 NESCOR Failure Scenarios[19]

The NESCOR Failure Scenarios document provides a resource for utilities to gain an understanding of cyber security risks and potential mitigations in various functional domains. The material is designed to support risk assessment, policies, planning, procedures, procurement, training, tabletop exercises and security testing.

The information about potential cyber security failure scenarios is intended to be useful to utilities for risk assessment, planning, procurement, training, tabletop exercises and security testing. A cyber security failure scenario is a realistic event in which the failure to maintain confidentiality, integrity, and/or availability of sector cyber assets creates a negative impact on the generation, transmission, and/or delivery of power. Some of the scenario descriptions include activities that typically are not allowed by policies, procedures, or technical controls. These scenarios may be used to ensure that the applicable mitigation strategies are specified and implemented.

The failure scenarios are organized in six categories, corresponding to the domains identified in the National Institute of Standards and Technology (NIST) Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0,* Office of the National Coordinator for Smart Grid Interoperability.

1. Advanced Metering Infrastructure (AMI)
2. Distributed Energy Resources (DER)
3. WAMPAC (Wide Area Monitoring, Protection, and Control)
4. Electric Transportation (ET)
5. Demand Response (DR)
6. Distribution Grid Management (DGM)
7. Generation (GEN)

In addition, there are failure scenarios in one additional category: Generic. Generic includes failure scenarios that may impact many of these functional domains.

Failure scenarios include malicious and non-malicious cyber security events such as:

- Failures due to compromising equipment functionality,
- Failures due to data integrity attacks,
- Communications failures,
- Human error,
- Interference with the equipment lifecycle, and
- Natural disasters that impact cyber security posture.

[19] url: smartgrid.epri.com/nescor.aspx

The failure scenarios included in the document are not intended to be a complete list of all possible failure scenarios, and their mitigations are a suggested list of recommendations intended to provide a variety of options. The scenario write-ups are brief, and commonly include specific details to aid understanding. This is in contrast to a single more general failure scenario that includes significant details to address all elements.

Included below is one of the scenarios. The italicized text are the common vulnerabilities and mitigations. These are standardized across all the scenarios.

Generic.1 Malicious and Non-malicious Insiders Pose Range of Threats

Description: Authorized personnel - who may be operators, engineering staff or administrators, become active threat agents with legitimate access to IT, field systems, and/or control networks.

Relevant Vulnerabilities:

- *Users and hardware/software entities are given access unnecessary for their roles* to perform duties that should be separated,
- *System permits unauthorized changes,*
- *Users lack visibility of unapproved access** when privileges are elevated for access to security-relevant or operationally critical functions,
- *Speed of incident response process is not appropriate for incident*.

Impact:

- Authorized personnel with legitimate access can inflict significant damage on a system either intentionally or by mistake. The impact for this scenario could range from a minor system being offline to a widespread outage of unknown duration.

Potential Mitigations:

- *Require separation of duty*,
- *Use role-based access control (RBAC)* to limit access,
- *Detect abnormal behavior* including out-of-policy behavior by authorized users in control networks through protection mechanisms and situational awareness, SIEM, intrusion detection system (IDS), firewalls, logging, and monitoring),
- *Define procedures* for processing suspected or confirmed security incidents involving an insider,
- *Define procedures* concerning access to security-relevant and operationally critical functionality.

5.4 Cybersecurity Capability Maturity Model (C2M2)[20]

The following content is extracted from the Department of Energy (DOE) *Cyber Security Capability Maturity Model* (C2M2) document.

[20] Department of Energy, *Cyber Security Capability Maturity Model (C2M2), Version 1.1,* February 2014.

Repeated cyber intrusions into organizations of all types demonstrate the need for improved cybersecurity. Cyber threats continue to grow and represent one of the most serious operational risks facing modern organizations. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. Beyond critical infrastructure, the economic vitality of the nation depends on the sustained operation of organizations of all types. The C2M2 can help organizations of all sectors, types, and sizes evaluate and make improvements to their cybersecurity programs.

The C2M2 focuses on the implementation and management of cybersecurity practices associated with the information technology (IT) and operations technology (OT) assets and the environments in which they operate. The model can be used to:

- Strengthen organizations' cybersecurity capabilities
- Enable organizations to effectively and consistently evaluate and benchmark cybersecurity capabilities
- Share knowledge, best practices, and relevant references across organizations as a means to improve cybersecurity capabilities
- Enable organizations to prioritize actions and investments to improve cybersecurity

The C2M2 is designed for use with a self-evaluation methodology and toolkit (available by request) for an organization to measure and improve its cybersecurity program.1 A self-evaluation using the toolkit can be completed in one day, but the toolkit could be adapted for a more rigorous evaluation effort. Additionally, the C2M2 model can inform the development of a new cybersecurity program.

The C2M2 provides descriptive rather than prescriptive guidance. The model content is presented at a high level of abstraction, so that it can be interpreted by organizations of various types, structures, sizes, and industries. Broad use of the model by a sector can support benchmarking of the sector's cybersecurity capabilities.

5.4.1 Model Architecture

The model arises from a combination of existing cybersecurity standards, frameworks, programs, and initiatives. The model provides flexible guidance to help organizations develop and improve their cybersecurity capabilities. As a result, the model practices tend to be at a high level of abstraction, so that they can be interpreted for organizations of various structures and sizes.
The model is organized into 10 domains. Each domain is a logical grouping of cybersecurity practices. The practices within a domain are grouped by objective - target achievements that support the domain. Within each objective, the practices are ordered by Maturity Indicator Level (MIL).

5.4.1.1 Domains

Each of the model's 10 domains contains a structured set of cybersecurity practices. Each set of practices represents the activities an organization can perform to establish and mature capability in the domain. For example, the Risk Management domain is a group of practices that an organization can perform to establish and mature cybersecurity risk management capability.

For each domain, the model provides a purpose statement, which is a high-level summary of the intent of the domain, followed by introductory notes, which give context for the domain and

introduce its practices. The purpose statement and introductory notes offer context for interpreting the practices in the domain. Following is a list of the domains:

Risk Management
Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

Asset, Change, and Configuration Management
Manage the organization's IT and OT assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.

Identity and Access Management
Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

Threat and Vulnerability Management
Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

Situational Awareness
Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other model domains, to form a common operating picture (COP).

Information Sharing and Communications
Establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience, commensurate with the risk to critical infrastructure and organizational objectives.

Event and Incident Response, Continuity of Operations
Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

Supply Chain and External Dependencies Management
Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

Workforce Management
Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

Cybersecurity Program Management
Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns

cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

6 REFERENCES

1. Michael J. Assante and Robert M. Lee, *The Industrial Control System Cyber Kill Chain,* October 5, 2015.

2. Center for Internet Security, *CIS Controls, V7,* 2018.

3. Crowd Research, *Insider Threat, 2018 Report.*

4. CrowdStrike, 2019 *Global Threat Report, Adversary Tradecraft and the Importance of Speed*, 2019.

5. Dragos, *Year in Review 2018, ICS Activity Groups and the Threat Landscape.*

6. Dragos, *Year in Review 2018, Industrial Control System Vulnerabilities.*

7. Dragos, *Year in Review 2018, Lessons Learned from Threat Hunting & Responding to Industrial Intrusion.*

8. ISO/IEC, *Information technology - Security techniques - Information security management systems – Requirements*, Second edition, 2013-10-01.

9. Lee, A., *Cyber Security Strategy Guidance for the Electric Sector*, EPRI, Palo Alto, CA: 2012. 1025672.

10. Lee, A., Rick Management in Practice: A Guide for the Electric Sector. EPRI, Palo Alto, CA: 2014. 3002003333.

11. National Electric Sector Cybersecurity Organization Resource (NESCOR), Electric Sector Failure Scenarios and Impact Analyses, Version 2.0, December 2015.

12. SANS, The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns, 2018.

13. Blake E. Strom, Joseph A. Battaglia, Michael S. Kemmerer, William Kupersanin, Douglas P. Miller, Craig Wampler, Sean M. Whitley, Ross D. Wolf, Finding Cyber Threats with ATT&CK™-Based Analytics, MITRE Technical Report 170202, June 2017.

14. Measuring & Managing the Cyber Risks to Business Operations, sponsored by Tenable, Independently conducted by Ponemon Institute LLC, Publication Date: December 2018.

15. U.S. Department of Energy, Cyber Security Capability Maturity Model (C2M2), Version 1.1, February 2014.

16. U.S. Department of Energy (DOE), Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), Version 1.1, February 2014.

7 POWER SUPPLY AND OUTAGE REGULATIONS

7.1 Georgia Accidental Power Outage Regulations

- In case of accidental power outage (caused by any reason), if disconnection continues more than 3 hours, utility has to inform all disconnected customers (by sms, email) about approximate time of reconnection
- If more than 2% of customer are without power (in particular area - city, village), the corresponding information should appear on company's web-page
- Maximum in 12 hours power should be supplied to customer (if it is not caused by external factors). In case of external factor (not depending on utility), utility should send to regulator corresponding approval documentation.

7.2 Resolution of the National Commission on Approval of the Procedure for Ensuring the Standards of Electricity Supply and Compensation to Consumers for their Non-Compliance

Common DSO's quality standards for the delivery of services include:

Call center service level within 30 seconds (percentage of calls connected to the call center operator within 30 seconds) in the reporting year - not less than 75%; the percentage of call center calls lost in the reporting year is no more than 10%.

Guaranteed DSO's quality standards include:

1) Observance of indicators of change of a voltage established by the Code of distribution systems;

2) Elimination of the reasons for non-compliance with electricity quality indicators based on the results of the consumer complaint (claim) regarding the quality of electricity from the day following the day when the DSO became aware of non-compliance with the electricity quality indicators by the measurement results, or from the day following the day of receipt of the complaint (claim) of the consumer if the DSO already knew the reasons for non-compliance with the electricity quality indicators: within a period of 30 days, if they can be eliminated by the operative actions of the personnel of the DSO; within 180 days in case of need for construction works or replacement of network elements;

3) Consideration of the complaint (claim) of the consumer regarding the quality of electricity with the information specified in clause 13.2.2 of Chapter 13.2 of Section XIII of the Distribution Systems Code, from the date of receipt of the complaint (claim): within a period of 15 days without measuring the quality parameters of electricity at the point of distribution to the consumer; within 30 days in the case of measurements of electricity quality parameters at the point of distribution to the consumer;

4) Renewal of power supply after the start of power supply interruption within 24 hours;

5) Issuance of technical specifications for new network connection together with the draft agreement on connection from the date of registration of the application for new network connection: within 10 business days for standard connection; within 10 working days for non-standard connection without the need to agree specifications with the transmission system operator; within 20 working days for non-standard connection if the technical conditions are agreed with the transmission system operator;

6) Submitting operating voltage for testing customer's electrical equipment from the date of receipt of the application with a complete package of documents to be attached to the application in accordance with the requirements of the Code of distribution systems: within 5 working days, if the power supply does not require interruption of power supply to other Users; within 10 working days, if the voltage supply requires interruption of the power supply to other Users;

7) Connecting customer's electrical installations to the electrical network from the date of receipt of the application: within 5 working days, if the connection does not require interruption of power supply to other Users; within 10 working days, if the connection requires interruption of electricity supply to other Users;

8) Issue of a paper copy of the signed agreement on the provision of distribution services within 3 working days from the date of receipt of the relevant request from the consumer;

9) issuance of the Passport of the point of distribution signed by the DSO within 10 working days from the date of receipt of the relevant request from the consumer;

10) Renewal of power supply of the electrical installation of the consumer, which was disconnected at the request of the consumer, within 5 working days from the date of providing by the consumer with documents confirming payment of the licensee services for restoration of power supply;

11) Renewal of the power supply of the consumer electrical installation, which was disconnected at the initiative of the DSO, from the date of providing the consumer with confirmation of elimination of detected violations, payment of arrears for services rendered and / or unauthorized selection of electricity, as well as compensation for losses (if any): in the urban area - within 3 business days; in rural areas - within 5 working days;

12) Restoration of power supply of the electrical installation of the consumer, which was disconnected at the request of the electricity supplier, from the date of receipt from the electricity supplier of information on elimination of the reasons for the power outage: in the urban area - within 3 business days; in rural areas - within 5 working days;

13) Verification of the meter within 20 days from the date of receipt of the relevant application from the consumer;

14) Consideration of appeals / complaints / claims consumers of receipt of appeals / complaints / claims of the consumer: within 30 days; within 45 days, if during the consideration of the appeal it is necessary to carry out a technical check or to carry out an examination of the means of metering of electricity;

15) Consideration of consumer requests for compensation for losses caused by DSO's failure to comply with electricity quality indicators within 30 days from the date of receipt of the request;

16) Consideration of consumer requests for checking the correctness of the invoice for electricity distribution services, if the provision of such invoices is provided for in the agreement on the provision of electricity distribution services with the consumer, within 5 working days from the date of receipt of the request.

8 ACRONYMS

APT	Advanced Persistent Threat
C2M2	Cybersecurity Capability Maturity Model
CIS	Center for Internet Security
DOE	Department of Energy
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
GDPR	General Data Protection Regulation
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IoT	Internet of Things
IIoT	Industrial Internet of Things
IT	Information Technology
MFA	Multifactor Authentication
MIL	Maturity Indicator Level
NCA	National Competent Authorities
NESCOR	National Electric Sector Cybersecurity Organization Resource
NIS Directive	The Directive on Security of Network and Information Systems
NIST	National Institute of Standards and Technology
OT	Operational Technology
PLC	Programmable Logic Controller
RBAC	Role-based Access Control
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Incident and Event Management

A GDPR AND NIS DIRECTIVE

Following are the assessments and fines that are applicable for non-compliance with the GDPR or the NIS Directive.

A.1 *GDPR Administrative fines*

The GDPR imposes fines on data controllers and processors for non-compliance.

A.1.1 *Determination*

Fines are administered by individual member state supervisory authorities (83.1). The following 10 criteria are to be used to determine the amount of the fine on a non-compliant firm:

- **Nature of infringement**: number of people affected, damaged they suffered, duration of infringement, and purpose of processing
- **Intention**: whether the infringement is intentional or negligent
- **Mitigation**: actions taken to mitigate damage to data subjects
- **Preventative measures**: how much technical and organizational preparation the firm had previously implemented to prevent non-compliance
- **History**: (83.2e) past relevant infringements, which may be interpreted to include infringements under the Data Protection Directive and not just the GDPR, and (83.2i) past administrative corrective actions under the GDPR, from warnings to bans on processing and fines
- **Cooperation**: how cooperative the firm has been with the supervisory authority to remedy the infringement
- **Data type**: what types of data the infringement impacts; see special categories of personal data
- **Notification**: whether the infringement was proactively reported to the supervisory authority by the firm itself or a third party
- **Certification**: whether the firm had qualified under approved certifications or adhered to approved codes of conduct
- **Other**: other aggravating or mitigating factors may include financial impact on the firm from the infringement

Each supervisory authority shall have all of the following corrective powers:

1. to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;

2. to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;

3. to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;

4. to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;

5. to order the controller to communicate a personal data breach to the data subject;

6. to impose a temporary or definitive limitation including a ban on processing;

7. to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;

8. to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

9. to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

10. to order the suspension of data flows to a recipient in a third country or to an international organisation.

A.1.2 ***Amount***

If a firm infringes on multiple provisions of the GDPR, it shall be fined according to the gravest infringement, as opposed to being separately penalized for each provision. (83.3). However, the above may not offer much relief considering the amount of fines possible:

A.1.2.1 Lower level

Up to €10 million, or 2% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements of:

- Controllers and processors under Articles 8, 11, 25-39, 42, 43
- Certification body under Articles 42, 43
- Monitoring body under Article 41(4)

A.1.2.2 Upper level

Up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher, shall be issued for infringements of:

- The basic principles for processing, including conditions for consent, under Articles 5, 6, 7, and 9
- The data subjects' rights under Articles 12-22

- The transfer of personal data to a recipient in a third country or an international organisation under Articles 44-49
- Any obligations pursuant to Member State law adopted under Chapter IX
- Any non-compliance with an order by a supervisory authority (83.6)

A.2 *NIS Directive – Sanctions: 2018 Status*

The following table summarizes the status of the sanctions that have been defined for non-compliance with the NIS Directive by members of the European Union. This table is current as of June 2018.

Country	Last reviewed	Sanctions regime
Austria	28.02.18	More details to follow.
Belgium	28.02.18	More details to follow.
Bulgaria	June 2018	Article 64 of the Electronic Government act provides for administrative fines ranging from BGN 500 up to BGN 3,000 in case of a violation of network and information security measures, committed or admitted by civil servants. In case of repeated violations the fines increase and shall range from BGN 1,000 up to BGN 5,000. Article 28 and Article 29 of the Cybersecurity Act (draft) provide for administrative fines ranging from BGN 30, 000 up to BGN 150,000 in case of failure to perform the reporting obligations under this Act. In case of a repeated violation the fines increase and shall range from BGN 150,000 up to BGN 300,000. Liability for other violations of the Act is also foreseen.
Croatia	28.02.18	More details to follow.
Cyprus	June 2018	Section 15 of the Draft Law provides that any person who prevents any employee of the competent authority to fulfil his duties is guilty of an offence and subject to imprisonment of up to 6 months and/or to a fine of up to EUR 8,000. Section 16 of the Draft Law provides that any person who breaches the Law, the regulations or the decisions of the competent authority is guilty of an offence and subject to imprisonment of up to 6 months and/or to a fine of up to EUR 8,000. Section 29 of the Draft Law provides for administrative fines of up to EUR 8,500 for violations of the Law or the decisions of the competent authority. The fine referred to in Article 15 and Article 16 of the Law is up to EUR 10.000 and not up to EUR 8.000. Article 30 of the Law provides for administrative fines of up to EUR 8,500 for violations of the Law or the decisions of the competent authority.
Czech Republic	28.02.18	Section 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 200,000, in particular in the following cases: Administrators or operators of the information or communication systems of a critical information infrastructure, administrators or operators of significant information systems or administrators and operators of the basic service information systems do not introduce/ carry out security measures or do not maintain security documentation. Providers of digital services do not introduce/ carry out security measures.

Country	Last reviewed	Sanctions regime
		Section 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 40,000, in particular in the following cases: Providers of electronic communication services, entities operating an electronic communication network or authorities or persons operating a significant network: do not fulfil their obligation imposed by the National Cyber and Information Security Agency contained in its decision or a measure of a general nature during a time of a cyber threat; or do not fulfil any of the obligations imposed through a corrective measure. Administrators and operators of the information or communication systems of critical information infrastructure or administrators or operators of significant information systems: do not report a cyber security incident; do not fulfil their obligation imposed by the National Cyber and Information Security Agency contained in its decision or a measure of a general nature; or do not hand over data, operating data and information. Administrators of the information or communication systems of critical information infrastructure or administrators of a significant information system do not notify the operator of the system. Administrators or operators of the information or communication systems of critical information infrastructure do not notify the entities operating an electronic communication network. Operators of the information or communication systems of critical information infrastructure: do not fulfil their obligation imposed by the National Cyber and Information Security Agency contained in its decision; do not hand over data, operating data and information; or do not destroy copies of data, operating data and information. Authorities or persons operating a significant network do not report a cyber security incident. Administrators and operators of the basic service information systems: do not report a cyber security incident; do not fulfil its obligation to inform the public imposed by the National Cyber and Information Security Agency; do not fulfil an obligation imposed by the National Cyber and Information Security Agency; or do not fulfil an obligation imposed through a corrective measure. Administrators or operators of the information or communication systems of a critical information infrastructure, administrators or operators of the significant information systems, administrators or operators of the basic service information systems and operators of basic services, who are public authorities, enter into a contract with a provider of cloud computing services.

Country	Last reviewed	Sanctions regime
		Administrators or operators of the information or communication systems of critical information infrastructure do not fulfil their obligation to notify the public imposed by the National Cyber and Information Security Agency. Operators of basic services: do not notify the administrators or providers of basic service information systems; do not report a significant impact on the continuity of provision of the basic service whether or not caused by a cyber security incident; or do not fulfil its obligation to inform the public imposed by the National Cyber and Information Security Agency. Providers of digital services: do not appoint their representative; do not report a cyber security incident; or do not fulfil its obligation to inform the public imposed by the National Cyber and Information Security Agency. Section 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 8,000, in particular in the following cases: Operators of the information or communication systems of critical information infrastructure: do not hand over data, operating data and information; or do not allow administrators to supervise the destruction of data, operating data and information. Section 25 of the CSA provides for administrative fines to legal persons of up to approx. EUR 400, in particular in the following cases: Administrators or operators of the information or communication systems of critical information infrastructure or administrators or operators of significant information systems do not fulfil their obligation imposed by the National Cyber and Information Security Agency contained in its decision.
Denmark	28.02.18	Breaches will be sanctioned by way of fines, unless the breach in question is so serious that another, more stringent legislation applies to the specific situation.
Estonia	28.02.18	Section 19 of the CSA provides for administrative fines of up to EUR 20,000, where the security measures of service providers set out in section 7(1)-(3) of the CSA are not followed.
Finland	15.06.18	No proposed new sanctions; existing sanction regimes provided in the sector specific laws may apply.
France	28.02.18	At the moment, Article 9 of the Act provides for three criminal fines for the operators of essential services:

Country	Last reviewed	Sanctions regime
		directors that do not comply with the security rules even after the timeline specified in a formal demand issued by the ANSSI shall be punishable with a fine of €100,000; directors that do not comply with their reporting obligation in case of an incident shall be punishable with a fine of €75,000; directors that obstruct an investigation shall be punishable with a fine of €125,000. Article 15 of the Act provides for three criminal fines for the digital service providers: directors that do not comply with the security rules even after the timeline specified in a formal demand issued by the ANSSI shall be punishable with a fine of €75,000; directors that do not comply with their reporting obligation in case of an incident shall be punishable with a fine of €50,000; directors that obstruct an investigation shall be punishable with a fine of €100,000.
Germany	28.02.18	Section 14 of the FOIS Act provides for administrative fines of up to EUR 50.000, in particular in the following cases: Operators of critical infrastructures wilfully or negligently fail to properly implement appropriate technical and organisational measures to prevent disruptions of availability etc. in a timely manner fail to properly designate a point of contact in a timely manner fail to properly report as described above. Providers of digital services wilfully or negligently fail to implement technical and organisational measures to tackle risks for the security of the network and information systems fail to properly report as described above. Infringements of providers of digital services are only sanctioned by the German authorities, if the provider (i) has no main establishment in another EU member state, or (ii) where it has no establishment in another EU member state, has appointed a representative there and offers the digital services in that EU member state. Further, the Implementation Act amends the sanction rules under the Atomic Energy Act, Energy Industry Act, Social Insurance Code V and Telecommunication Act, whilst the administrative fines remain as before: up to EUR 50.000 under the Atomic Energy Act; up to EUR 5.000.000, or in specific cases up to 10% of the total worldwide annual turnover of the preceding financial year, under the Energy Industry Act; up to EUR 50.000 under the Social Insurance Code V; and up to EUR 500.000 under the Telecommunication Act.

Country	Last reviewed	Sanctions regime
Greece	28.02.18	More details to follow.
Hungary	28.02.18	Annex 1 of Government Decree 410/2017 (XII.15) on registration obligedservices provides for administrative fines to providers of registration- obliged services in case of breaching the obligations specified by the Annex of the Government Decree including the failure to notify the Directorate about significant incidents. The amount of the imposed fine depends on the type of breach of obligation and varies between HUF 50,000 (~ EUR 165) and HUF 5,000,000 (~ EUR 16,500). The amount of fine cannot exceed HUF 5,000,000 even in case of multiple breaches of obligations, however fines can be imposed for the same breach of obligations as well.
Ireland	28.02.18	More details to follow.
Italy	28.02.18	Please note that no specific sanction regimes at national level has been implemented yet since the NIS Directive has not been yet implemented. However, the National Plan establishes to set up and implement a standard for the evaluation of different damages in relation to the occurred cybernetic events. The law implementing the NISD in Italy should reasonably establish monetary and non-monetary penalties in case of cybernetic events of particular national relevance, and the relevant penalties in case of omission of notification obligations.
Latvia	28.02.18	More details to follow.
Lithuania	28.02.18	No official information is made available publicly yet.
Luxembourg	28.02.18	More details to follow.
Malta	28.02.18	No information on this has, as yet, been made publicly available.
Netherlands	28.02.18	The draft Cybersecurity Act provides for the following administrative fines: up to EUR 5 million for any breach of the Cyber Security Act by essential service operators or digital service providers; a maximum of EUR 1 million for failing to cooperate with a request for further information from the National Cyber Security Centre; and a maximum fine of EUR 1 million for failure to adequately cooperate with supervisory authorities exercising their competencies.
Poland	28.02.18	Article 57 of the NCSA provides for administrative fines of up to PLN 200,000 (EUR 50,000) imposed by the competent authority, in particular in the following cases: Operators of critical infrastructure fail to implement a security management system, ensuring management of incidents, including their identification, classification and prioritisation of incident handling, registration, analysis,

Country	Last reviewed	Sanctions regime
		searching for connections, undertaking corrective actions and remedying the causes of incidents and providing information on serious incidents to the appropriate CSIR; fail to classify security incidents; fail to properly report a significant incident. If as a result of an inspection the competent authority finds that an operator of critical infrastructure persistently violates the Act, causing: a direct and serious threat to cybersecurity for defence, state security, public safety and order, or human life and health; the threat of serious damage to property or serious difficulties in providing key services; the competent authority will impose a penalty of up to PLN 200,000.
Portugal	28.02.18	More details to follow.
Romania	28.02.18	Failure to comply with the prescribed obligations may be sanctioned with administrative fines ranging from RON 3,000 (approx. EUR 670) to RON 50,000 (approx.EUR 11,000). Repeated breaches of the obligations may be sanctioned with administrative fines of up to RON 100,000 (EUR 22,000). Companies with a turnover exceeding RON 2,000,000 (approx. EUR 440,000), may be subject to the administrative fines of up to 2% of the company's turnover and, for repeated breaches, of up to 5% of the company's turnover.
Slovakia	28.02.18	The authority can impose a fine on a natural person of EUR 100- EUR 5,000. The legal entity/operator of the essential services or a digital service provider may be sanctioned and fined between EUR 300 and 1% of annual turnover (provided it does not exceed EUR 300,000). The authority will also be authorised to impose fines between EUR 300 and EUR 100,000 to anyone, who does not provide the required information relating to national cyber security strategy. When determining the amount of fines, the authority will take into account the seriousness of the administrative offense/tort, in particular the manner of committing it, the duration, consequences and circumstances in which it was committed (Sections 30 and 31).
Slovenia	28.02.18	Article 38 of the draft bill provides for fines in misdemeanour proceedings from EUR 500 to EUR 10,000 for medium and large companies, in particular in the following cases: Operators of essential services fail to properly designate a point of contact in a timely manner fail to implement appropriate technical and organisational measures to prevent disruptions of availability etc. fail to properly report a security incident

Country	Last reviewed	Sanctions regime
		fail to properly implement a decision of competent national authority. Article 39 of the draft bill provides for fines in misdemeanour proceedings from EUR 10,000 to EUR 50,000 for medium and large companies and from EUR 500 to EUR 10,000 for other companies, in particular in the following cases: Providers of digital services fail to implement technical and organisational measures to tackle risks for the security of the network and information systems fail to properly report a security incident. Article 40 of the draft bill provides for fines in misdemeanour proceedings from EUR 200 to EUR 2,000, in particular in the following cases: The responsible person of the state administration authority fails to implement appropriate technical and organisational measures to prevent disruptions of availability. fails to properly report a security incident fails to properly implement the decision of competent national authority.
Spain	28.02.18	Article 36 of the draft law includes information relating to breaches of the draft law. Infringements are categorised as very serious, serious or minor infringements. A very serious breach would be, for example, the repeated breach of the obligation to report incidents. A serious infraction would be, for example, a breach of the obligation to report incidents with significant impact on services. A minor breach would be, for example, a breach of the obligation to report incidents without significant impact on services. The draft includes the following penalties which apply in case of an infringement (Article 37): (i) fines of EUR 500,001 to EUR 1,000,000 for very serious infringements; (ii) fines of EUR 100,001 to EUR 500,000 for serious infringements, and warnings or fines of up to EUR 100,000 for minor infringements. The sanctioning body will determine the sanctions based on criteria established in the draft law, such as the degree of culpability, number of users affected or the volume of billing of the offender.
Sweden	28.02.18	If the relevant authority finds that the supplier does not comply with the act or ordinance they can instruct the supplier to take action. The request can be combined with a penalty fine. Further, the relevant regulatory authority will decide on administrative fines from 5,000 SEK to 10,000,000 SEK for not complying with the security requirements or incident notification.
United Kingdom	03.05.18	The Government proposes that the penalty regime for the NIS Directive will include a maximum financial penalty of £17m, which will cover all contraventions, such as (for example) failure to cooperate with the competent authority, failure to report a reportable incident, failure to comply

Country	Last reviewed	Sanctions regime
		with an instruction from the competent authority, failure to implement appropriate and proportionate security measures. Financial penalties will only be levelled as a last resort where it is assessed appropriate risk mitigation measures were not in place without good reason. In addition, the maximum penalties should be reserved for the most severe cases, , and it is expected that mitigating factors (including steps taken to comply with the NIS Directive, actions taken to remedy any consequences) and sector specific factors will be taken into account by the competent authority when deciding appropriate regulatory response. In the event of any enforcement action by the competent authority, it will notify the operator of impending action, allow the operator an opportunity to make representations, and confirm the final decision and reasoning of the competent authority. Decisions taken by the competent authority will be enforceable by civil proceedings, and appealable through the court system. It is also proposed that breach of the NIS Directive is cumulative with any GDPR sanction. There may be reason for an operator to be penalised under different regimes for the same event because the penalties might relate to different aspects of the wrongdoing and different impacts. However, the NIS Regulations will include text which will encourage competent authorities to work with regulators in the event of different regimes applying to determine what approach to take. This will not limit a competent authority's ability to apply the penalty it feels is appropriate to the circumstances, but will encourage it to factor in other regimes if this is appropriate.

B SAMPLE FAILURE SCENARIO AND SCORING

This example illustrates scoring a scenario for a system and ranking it on the risk graph. The system is a transmission substation and is called System 1. (Note: to develop an accurate assessment of each system, multiple scenarios should be scored.)

Generic.4a Supply Chain Attacks Weaken Trust in Equipment

Description: An adversary replaces a legitimate device with a maliciously altered device and introduces the device into the supply chain without directly compromising a manufacturing entity. This can be done by buying a legitimate device, buying or creating a malicious device and returning the malicious device in place of the legitimate device as an exchange. Alteration may be a modification or deletion of existing functions or addition of unexpected functions.

Relevant Vulnerabilities:

- *System permits unauthorized changes* in the supply chain.

Impact:

- Depending on the level of sophistication of the threat agent, this scenario can result in the complete loss of integrity and availability of systems using equipment from an infiltrated supply chain.

Potential Mitigations:

- *Develop SLA* for procurement which verifies the manufacture and origin of equipment from a known good and reputable source,
- *Perform audit* of the supply chain periodically, to ensure adequate quality control,
- *Detect abnormal behavior* that may indicate supply chain issues, such as unauthorized communications or behavior by deployed devices in the system network,
- *Test before installation*, to detect unwanted functionality before putting devices into production. The objective is to validate functionality and usability.

The assumption is that the impact is for a small geographic area with a loss of data/command integrity. The cyber attack is a result of a replaced device that included malicious code. As specified below, there are some criterion that are assessed as N/A, because they are not applicable. The utility has decided to include all the Impact criteria and mark some as N/A, as appropriate. Therefore, the maximum Impact score would be 99.

Table 3: Sample Impact Scores for the Generic.4 Scenario

Criterion	How to score	Score
System scale	0: single utility customer, 1: small geographic area, 3: town or city, 9: potentially full utility service area and beyond	1

Criterion	How to score	Score
External customers, e.g., other utilities	0: none, 1: high voltage customer, power generator, 3: DSO, 9: transnational interconnections, ENTSO-E interconnected systems	1
Public safety concern	0: none, 1: 1-20 injuries possible, 3: 100 injured possible, 9: one death possible	N/A
Workforce safety concern	0: none, 3: any possible injury, 9: any possible death	3
Ecological concern	0: none, 1: local ecological damage such as localized fire or spill, repairable, 3: permanent local ecological damage, 9: widespread temporary or permanent damage to one or more ecosystems such as the Exxon Valdez or Chernobyl	0
Financial impact of compromise on utility	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%	3
Restoration costs - cost to return to normal operations, not including any ancillary costs	0: Petty cash or less, 1: < 1% of utility organization O&M budget, 3: <=10%, 9: > 10%	3
Negative impact on generation	0: No effect, 1: Small generation facility off-line or degraded operation of large facility, 3: More than 10% loss of generation for 8 hours or less, 9: More than 10% loss of generation for more than 8 hours	N/A
Negative impact on the energy market	0: No effect, 1: localized price manipulation, lost transactions, loss of market participation 3: price manipulation, lost transactions, loss of market participation impacting a large metro area, 9: market or key aspects of market non-operational	N/A
Negative impact on the bulk transmission system	0: No effect, 1: loss of transmission capability to meet peak demand or isolate problem areas, 3: Major transmission system interruption, 9: Complete operational failure or shut-down of the transmission system	1
Negative impact on customer service	0: No effect, 1: up to 4 hour delay in customer ability to contact utility, and gain resolution, lasting one day, 3: up to 4 hr. delay in customer ability to contact utility and gain resolution, lasting a week, 9: more than 4 hr. delay in customer ability to contact utility and gain resolution, lasting more than a week	N/A
Negative impact on billing functions	0: None, 1: isolated recoverable errors in customer bills, 3: widespread but correctible errors in bills, 9: widespread loss of accurate power usage data, unrecoverable	N/A
Destroys goodwill toward utility	0: No effect, 1: negative publicity but this doesn't cause financial loss to utility, 3: negative publicity causing up to 20% less interest in advanced programs, 9: negative publicity causing more than 20% less interest in advanced programs; loss of major accounts	1

Criterion	How to score	Score
Immediate economic damage - refers to functioning of society as a whole	0: none, 1: local businesses down for a week, 3: regional infrastructure damage, 9: widespread runs on banks	0
Long term economic damage	0: none, 1: (not used), 3: several year local recession, 9: several year national recession	0
Causes a loss of privacy for a significant number of stakeholders	0: none, 1: 1000 or less individuals, 3: 1000's of individuals, 9: millions of individuals	N/A
GDPR Data Protection Violation	0: no violation, 1: minor violation, 3: clear violation, 9: significant violation	N/A
Legal Liability	0: Petty cash or less, 1: up to 2% of utility revenue, 3: up to 5%, 9: Greater than 5%	1
NIS Directive Non-Compliance	0: no violation, 1: minor violation, 3: clear violation, 9: significant violation	N/A
Total - impact		11

Following are the Likelihood and Opportunity Criteria Scores for System 1. The threat likelihood should be determined based on the tailored scenario. Because all likelihood and opportunity criteria are applicable, the maximum score is 81.

Table 4: Sample Likelihood and Opportunity Scores for the Generic.4 Scenario

Criterion	How to score	Score
Skill required	0: Deep domain/insider knowledge and ability to build custom attack tools, 1: Domain knowledge and access to cyber attack techniques, 3: Special insider knowledge needed, 9: Basic domain understanding and computer skills	1
Accessibility (physical)	0: Inaccessible, 1: Guarded, monitored, 3: Fence, standard locks, 9: Publicly accessible	0
Accessibility (logical, assume have physical access)	0: High expertise to gain access, 1: Not readily accessible, 3: Publicly accessible but not common knowledge, 9: Common knowledge or none needed	0
Attack vector - ease of exploit (assume have physical and logical access)	0: Theoretical, 1: Similar attack has been described, 3: Similar attack has occurred, 9: Straightforward, script or tools available	1
Attack vector – ease of discovery by threat agents	0: Extremely difficult, 1: Difficult, 3: Easy, 9: Publicly known	1
Attack vector – awareness by threat agents	0: Unknown, 1: Hidden/difficult to find, 3: Obvious, 9: Publicly known	2
Occurrence of vulnerability	0: Isolated occurrence, 1: More than one utility, 3: Half or more of power infrastructure, 9: Nearly all utilities	1

Criterion	How to score	Score
Motivation	0: No reward; 1: Possible reward, 3: Low reward, 9: High reward	3
Size/coordination of threat agents	0: Nation state/criminal organization, 1: Developers, partners, administrators, 3: Compromised internal account/user, 9: Local access by Internet user	1
Total – effects on likelihood and opportunity		**10**

The overall risk is based on the severity of the specific attack. Because both sets of scores are low, System 1 is ranked in the lower right quadrant, as illustrated in the figure below.

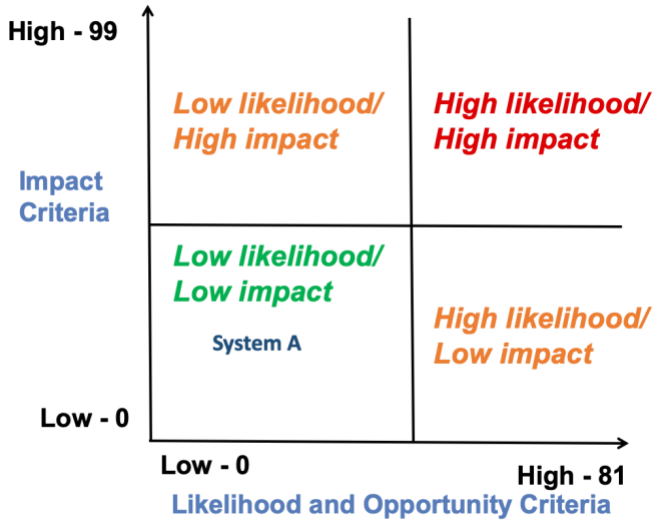

Figure 15: Ranking of System 1 Using the Scenario

If the risk is not acceptable, the utility should select the potential mitigation strategies. For this scenario, the selected mitigation strategies are:

- *Perform audit* of the supply chain periodically, to ensure adequate quality control,
- *Test before installation*, to detect unwanted functionality before putting devices into production. The objective is to validate functionality and usability.

Once the mitigation strategies are implemented, another risk assessment should be performed. The objective is to validate the effectiveness of the controls.