2018 IEEE Symposium on Security and Privacy Workshops

Insider Threat Cybersecurity Framework Webtool & Methodology: Defending Against Complex Cyber-Physical Threats

Michael Mylrea, Sri Nikhil Gupta Gourisetti, *Member, IEEE*, Curtis Larimer, Christine Noonan
Pacific Northwest National Laboratory
michael.mylrea@pnnl.gov, srinikhil.gourisetti@pnnl.gov, curtis.larimer@pnnl.gov, christine.noonan@pnnl.gov

Abstract— **This paper demonstrates how the Insider Threat Cybersecurity Framework (ITCF) web tool and methodology help provide a more dynamic, defense-in-depth security posture against insider cyber and cyber-physical threats. ITCF includes over 30 cybersecurity best practices to help organizations identify, protect, detect, respond and recover to sophisticated insider threats and vulnerabilities. The paper tests the efficacy of this approach and helps validate and verify ITCF's capabilities and features through various insider attacks use-cases. Two case-studies were explored to determine how organizations can leverage ITCF to increase their overall security posture against insider attacks. The paper also highlights how ITCF facilitates implementation of the goals outlined in two Presidential Executive Orders to improve the security of classified information and help owners and operators secure critical infrastructure. In realization of these goals, ITCF: provides an easy to use rapid assessment tool to perform an insider threat self-assessment; determines the current insider threat cybersecurity posture; defines investment-based goals to achieve a target state; connects the cybersecurity posture with business processes, functions, and continuity; and finally, helps develop plans to answer critical organizational cybersecurity questions. In this paper, the webtool and its core capabilities are tested by performing an extensive comparative assessment over two different high-profile insider threat incidents.**

Keywords—*Insider threat; cybersecurity framework; vulnerability assessment; cybersecurity web tool; cybersecurity methodology*

I. Introduction

All organizations face security risks. In 2011, former President Obama issued Executive Order (E.O.) 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information [1]. This was quickly followed in 2012 by the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs [2]. The Order and the Policy provide additional guidance for the development of insider threat programs in federal agencies to improve the security of classified information on computer networks. Despite the formulation of an insider threat strategy and policy, federal agencies nonetheless still grapple with how to implement their own programs and in the process, better understand the human and organizational issues surrounding the insider threat problem. As of 2016, 23% of electronic crime events were suspected or known to be caused by insiders [3]. Insider attacks can be technically sophisticated or markedly low-tech and have caused significant damage to organizations across sectors. More than 1000 cases of significant malicious insider activity have been documented with fraud, sabotage, and theft of intellectual property being the most common forms [4]. An average organization can expect to spend $4.3 million annually to mitigate, address, and resolve insider threats [5]. Overall, insider threats inflict $40 billion in losses across the US economy [6]. Several high-profile incidents perpetrated by insiders have raised the level of attention given to this important issue. Directed by E.O. 13587 and the National Insider Threat Policy, the National Insider Threat Task Force is responsible for the development of the United States government-wide policy for the deterrence, detection, and mitigation of insider threats [7]. This paper presents the Insider Threat Cybersecurity Framework (ITCF), which is designed to address various insider threat challenges that increasingly threaten organization owners and operators.

The following sections will demonstrate the ITCF webtool; a maturity model with four levels of increasing maturity, each level embedded in the one above, that address measures to address security in five domains of defense: (1) identify, (2) detect, (3) protect from, (4) respond to, and (5) recover from an insider attack. The webtool's dashboard displays that provide a window into the level of preparedness across each of these five domains, data analytics capabilities are discussed in section-II and through the use cases in section-IV.

II. ITCF Webtool

The ITCF webtool was developed to provide a detailed set of guidelines to help organizations that own and operate critical infrastructures identify, detect, protect, respond and recover to emerging cyber-physical insider threats and vulnerabilities. This is especially challenging as modern critical infrastructure facilities weave together cyber-physical systems that are increasingly connected to the internet and are vulnerable to complex, non-linear and evolving cyber threats [8]. The ITCF helps operators understand the cybersecurity posture and maturity of those complex connected systems. The ITCF is also designed to meet the goals of E.O. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [9, 10]. The ITCF is available online at www.cybersecfw.org (a passphrase may be requested from the authors).

The ITCF webtool is complemented by a "how-to" document that discusses the roles of the cybersecurity domains and their respective core elements in managing cybersecurity

This study has been conducted at the Pacific Northwest National Laboratory is operated for the U. S. Department of Energy by the Battelle Memorial Institute under Contract DE-AC05-75RL01830.

DOI 10.1109/SPW.2018.00036

risks for organizations, the details are described in [11, 12]. The ITCF also has the capability to compare the current and post-cybersecurity posture of an organization before and after cyber mitigations, assessments, and investments. Such capability is vital for efficient security management and to make business continuity decisions based on cybersecurity investments [13]. Moreover, this feature helps answers several critical questions that most cybersecurity assessment tools fail to answer: What is my return on investment? Where should I focus my cybersecurity investments? What are the "low hanging fruit" or areas that my organization can secure today in absence of additional resources? Answering these questions is imperative to establish a cybersecurity value proposition for any tool or methodology.

The ITCF is organized into five domains: Identify, Protect, Detect, Respond and Recover. These domains are further classified into their unique organizational blocks (or core elements or sub-domains), each of which has a set of questions, termed as core-checklist. The core-checklist questions are divided into four Maturity Indicator Levels (MILs): MIL0, MIL1, MIL2, and MIL3. Every question has four options: Fully Implemented (FI): Complete, the practice is performed as in the Framework; Largely Implemented (LI): Complete, but with a recognized opportunity for improvement; Partially Implemented (PI): Incomplete, with multiple opportunities for improvement; Not Implemented (NI): Absent, the practice is not performed by the organization.

During assessments, diverse stakeholders, from an organization such as systems engineers, managers, IT and cybersecurity staff, are assembled to answer a set of critical questions based on industry best practices. Instead of physically reviewing best practices documents, many of which are often over 100 pages in length, the ITCF assessment distills key elements of each methodology and presents them as a simple questionnaire (sample questions can be seen in the Appendix). Assessments take about 2 hours on average and conclude with the generation of an automatically generated detailed assessment report identifying vulnerabilities and gaps based on responses to assessment questions. Next, identified vulnerabilities and gaps are analyzed and a list of prioritized mitigations are recommended. Using that information, an organization's management can develop a plan to eliminate security gaps, measure their current cybersecurity posture and compare different groups within an organization. To measure progress, it is recommended to repeat the assessment at least every six months. This process, tool, and methodology will help stakeholders, operators, and owners manage their cybersecurity risk and increase their cybersecurity organization posture.

A. Design and Features

The ITCF was built from the ground-up with a focus on ease of use and functionality. Some of the design features of the webtool include:

1. *Cybersecurity CORE:* This contains 100+ critical insider threat questions that are tailored towards technical and non-technical/management aspects of an organization. These are divided into five domains: Identify, Protect, Detect, Respond, and Recover that are further divided into sub-domains. The CORE framework questionnaire is inspired by a conglomerate of NIST cybersecurity standard documents and frameworks.
2. *Cybersecurity Checklist:* This checklist focuses technical and managerial aspects of the organization from high-level policy and procedures to component and device levels security controls. The checklist contains 200+ items.
3. *Cybersecurity Qualitative Risk Assessment:* This facilitates the organization owners to inventory their assets, estimate their vulnerability, impact. The tool generates a qualitative risk graph that estimates the risk category of an asset.
4. *Cybersecurity Compare Tool:* This lets the organization operators and owners compare the current assessment with any number of past assessments to analyze the overall improvement of the organization's cybersecurity posture.
5. *Cached Progress:* Responses to the assessment questions are saved in the browser cache. If needed, the assessment can be completed as time permits instead of in one sitting.
6. *Load/Save Progress:* The assessment progress can be saved to a file which facilitates comparison over time.
7. *Export PDF Report:* At the end of an assessment, the ITCF webtool generates a report with interactive graphics and data visualizations in the web portal. In addition, the report can also be exported as a .pdf file for portability.

The ITCF provides a core-checklist that includes a combined list of 200+ key insider threat questions and items that target various aspects of an organization's cybersecurity. Each question has four options signifying a degree of implementation level: a) Fully Implemented; b) Largely Implemented; c) Partially Implemented; d) Not Implemented. Based on the responses to the core-checklist questions, the ITCF webtool generates a detailed insider threat assessment report with identified vulnerabilities and gaps through a variety of data visualizations. This information can be used to prioritize the actions based on business processes to mitigate gap.

B. Data Visualizations

1. *Fluid Gauges:* The fluid gauges are a way of showing more specific data from the evaluation. Specific domains, or all domains can be selected with any combination of MILs. Throughout the ITCF webtool, the cybersecurity states in each visualization are color coded as: *green* for *fully implemented*, *blue* for *largely implemented*, *purple* for *partially implemented*, and *red* for *not implemented*

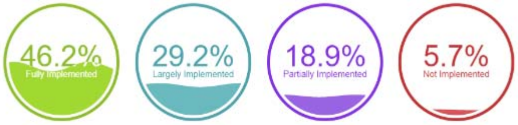


Fig. 1. Illustrative Fluid Gauge summary

2. *Pie Summary:* The pie summary is a brief overview of the evaluation results. The pies are organized by domain and MIL. By default, the pie summary is depicted as follows: MIL2 pie includes the responses to both MIL1 and MIL2 questions. Similarly, MIL3 pie includes the responses to MIL1, MIL2 and MIL3 questions. Although, the tool also generates a second version of this summary which does not combine lower MILs (independent pie summaries). In the

ITCF, MIL1 indicates that the initial practices performed may be in ad hoc manner; MIL2 indicates that the practices are documented, stakeholders are involved, and adequate resources are provided and used; MIL3 indicates that the procedures and systems are reviewed in conformance and are guided with policies. MIL3 also emphasizes on strict access controls, roles and responsibilities. Section III-A discusses more about the MILs.

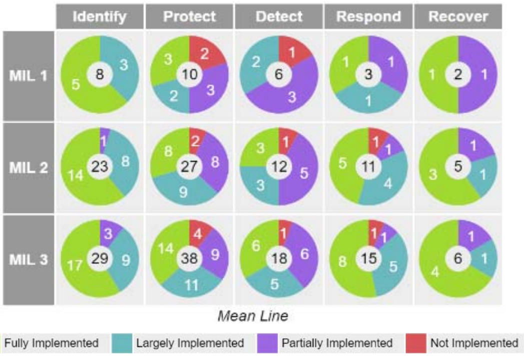


Fig. 2. Illustrative Pie summary

3. *Isometric Map:* The isometric map provides another method of visualizing the overall data. Various user interface options are provided to adjust the graphics. Some of those sub-features include changing the size and viewing angle of the organizations. In Fig.3, the domains (Identify, Protect, Detect, Respond, and Recover) and shows on the Y-axis, the cybersecurity states (Not Implemented to Fully Implemented) are shown on the X-axis. Section III discuses more about the domains.

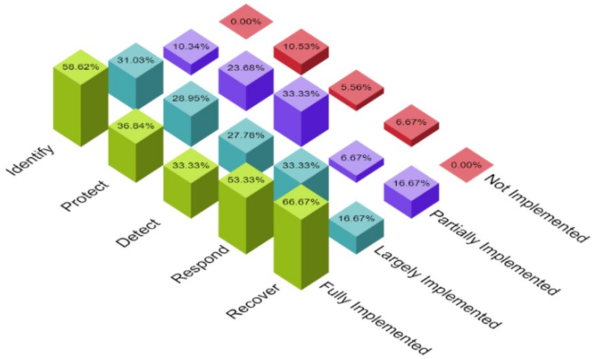


Fig. 3. Illustrative Isometric map with domains and cybersecurity states

4. *Cumulative Median Bar Graph:* The cumulative median bar graph provides a deeper method of data visualization. Through this, the owner/operator can see the median maturity level of each sub-domain in a domain. It is "cumulative" because in this case, MIL1 is subset of MIL2 and MIL2 is subset of MIL3.

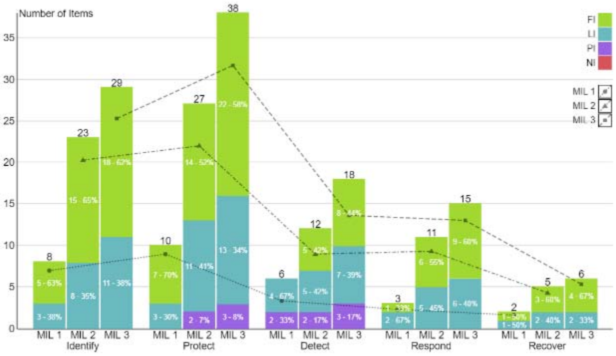


Fig. 4. Illustrative Cumulative median bar graph

5. *Maturity Indicator Level Gauge:* This visual helps the owner and operator see the status (cybersecurity posture) of the organization at each MIL.

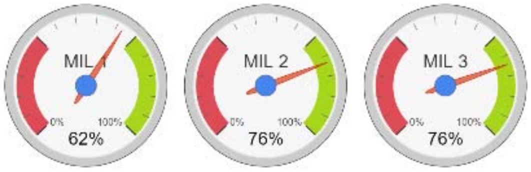


Fig. 5. Illustrative Maturity Indicator Level gauge

6. *Non-Cumulative Median Bar Graph:* The non-cumulative median bar graph provides a method of data visualization that is very similar to the cumulative median bar graph. Through this, the owner/operator can see the median maturity level of each sub-domain in a domain. It is "non-cumulative" because in this case, MIL1, MIL2 and MIL3 are independently represented.

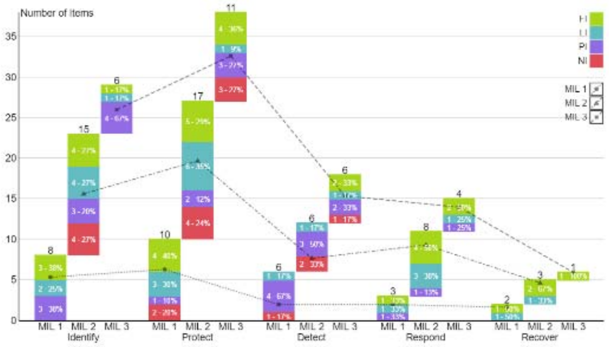
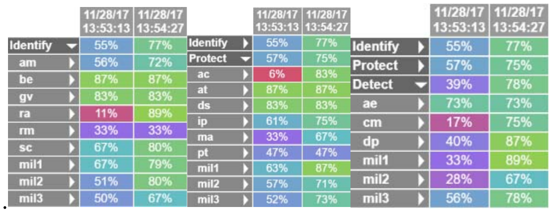


Fig. 6. Illustrative Non-Cumulative Median Bar Graph

7. *Comparative Summary Tables:* This summary table is generated from the "cybersecurity compare tool" plugin. When the owner/operator imports multiple assessment files, this plugin generates a tabular summary of maturity of each both domain and sub-domain level. This comparative analysis is shown in percentages.



	11/28/17 13:53:13	11/28/17 13:54:27
Identify ▼	55%	77%
am ▶	56%	72%
be ▶	87%	87%
gv ▶	83%	83%
ra ▶	11%	89%
rm ▶	33%	33%
sc ▶	67%	80%
mil1 ▶	67%	79%
mil2 ▶	51%	80%
mil3 ▶	50%	67%

	11/28/17 13:53:13	11/28/17 13:54:27
Identify ▶	55%	77%
Protect ▼	57%	75%
ac ▶	6%	83%
at ▶	87%	87%
ds ▶	83%	83%
ip ▶	61%	75%
ma ▶	33%	67%
pt ▶	47%	47%
mil1 ▶	63%	87%
mil2 ▶	57%	71%
mil3 ▶	52%	73%

	11/28/17 13:53:13	11/28/17 13:54:27
Identify ▶	55%	77%
Protect ▶	57%	75%
Detect ▼	39%	78%
ae ▶	73%	73%
cm ▶	17%	75%
dp ▶	40%	87%
mil1 ▶	33%	89%
mil2 ▶	28%	67%
mil3 ▶	56%	78%

Fig. 7. Illustrative Comparative Summary Tables

8. *Timeline Bar Graph:* This graph is generated from the "cybersecurity compare tool" plugin. When the owner/operator imports multiple assessment files, this plugin generates a bar graph with a "total implementation" line of maturity of all domains. The Y-axis for this graph is "percentage implemented".

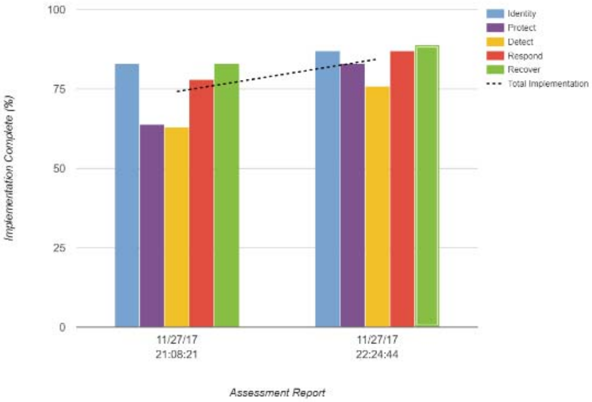
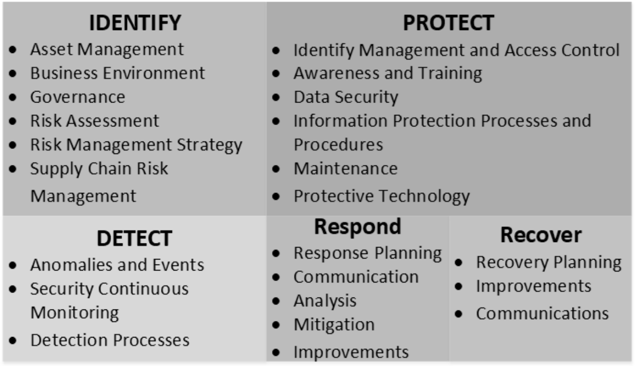


Fig. 8. Illustrative Timeline Bar Graph

III. ITCF Webtool Report Structure

The ITCF webtool generates a post-assessment report that shows the identified gaps and vulnerabilities, directions to develop a mitigation plan, along with options to visualize data. The core elements and the architectural background of the questions in ITCF are discussed in [11, 12]. Currently, our research team has been iterating with NIST in verifying the comprehensiveness of ITCF's questionnaire.



IDENTIFY
- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

PROTECT
- Identify Management and Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Maintenance
- Protective Technology

DETECT
- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond
- Response Planning
- Communication
- Analysis
- Mitigation
- Improvements

Recover
- Recovery Planning
- Improvements
- Communications

Fig. 9. Core elements of the ITCF (Critical domains and subdomains)

A. Maturity Indicator Levels

ITCF defines four maturity indicator levels (MIL), MIL0 through MIL3, which apply independently to each domain in the ITCF. Four aspects of the MILs are important for understanding and applying the ITCF.

The MILs apply independently to each domain. As a result, an organization using the ITCF may be operating at different MIL ratings in different domains. For example, an organization could be operating at MIL1 in one domain, MIL3 in another domain, and MIL2 in a third domain.

The MILs are cumulative within each domain; to earn a MIL in a given domain, an organization must perform all of the practices at that level and its predecessor level(s). For example, an organization must perform all of the domain practices in MIL1, MIL2 to achieve MIL2 in the domain. Similarly, the organization would have to perform all practices in MIL1, MIL2, MIL3 to achieve MIL3.

Establishing a target MIL for each domain is an effective strategy for using the ITCF to guide cybersecurity program improvement. Organizations should become familiar with the practices in the ITCF prior to determining target MILs. Gap analysis activities and improvement efforts should then focus on achieving those targets.

Striving to achieve the highest MIL in all domains may not be optimal. Companies should evaluate the costs of achieving a specific MIL against potential benefits, business objectives, and the organization's cybersecurity strategy. However, the ITCF was developed so that all companies, regardless of size, should be able to achieve MIL1 across all domains.

B. Using the Evaluation Results

The ITCF is meant to be used by an organization to identify and execute a cybersecurity risk management strategy to protect information technology (IT) and operational technology (OT) from insider threats. Fig. 10 summarizes the recommended approach for using the ITCF framework. An organization conducts an assessment; uses it to identify and analyze the vulnerabilities and gaps; prioritizes mitigation; establishes plans, and lastly, execute those plans to fill gaps. As plans are executed, objectives change, and the cybersecurity risk evolves, therefore the process is repeated.

To aid in the analysis of identified gaps, survey questions that were recorded as either *Partially Implemented* or *Not Implemented* are consolidated in "Summary of Identified Gaps" section of the webtool report. The detailed evaluation process is depicted in Fig. 10.

C. Summary of Identified Gaps

The ITCF is designed such that the questions also reflect the answer to the problem. Organization operators and owners can use this information to develop an organizational plan to increase their cybersecurity posture. This section of ITCF web tool report depicts all the *Partially Implemented* and *Not Implemented* questions for each of the five domains while displaying their MILs (see Table-I for an example). The organization's management can use this information to connect the existing posture with business processes, functions, and eventually, estimate the reflection on business continuity.

That information can also be used to find answers for critical resource allocation questions such as 1) What are the critical (based on security concerns) areas for this organization? 2) What kind of resources are available (both monetary and human) to invest in those areas? 3) What are the post-investment outcomes (another assessment)? 4) How do those investments reflect on business processes, functions, and continuity? 5) What is the improvement/diminishment in the organization's cybersecurity posture over a period (self-assessment and self-evaluation)? Answering those key questions may aid the organization to make cybersecurity decisions that could positively impact their business structure while estimating the long-term monetary benefits by investing resources up front. Future work will focus on developing capability to perform cost-benefit analysis to estimate return on investment relating to the identified gaps and vulnerabilities.

IV. ITCF Case Studies

This section presents two use cases based on recent insider threat related events. Specifics from those events are combined with a fictitious organization [14] with the goal of validating and verifying the efficacy of ITCF's methodology and capabilities. An ITCF assessment is performed on this organization to examine the cybersecurity posture and maturity level of the organization. In this section, an initial assessment is performed for each of the case studies. Then, the organization adapts to improve its security posture based on ITCF results to address specific cybersecurity gaps and a second assessment is performed. Finally, both the assessments are compared to depict differences.

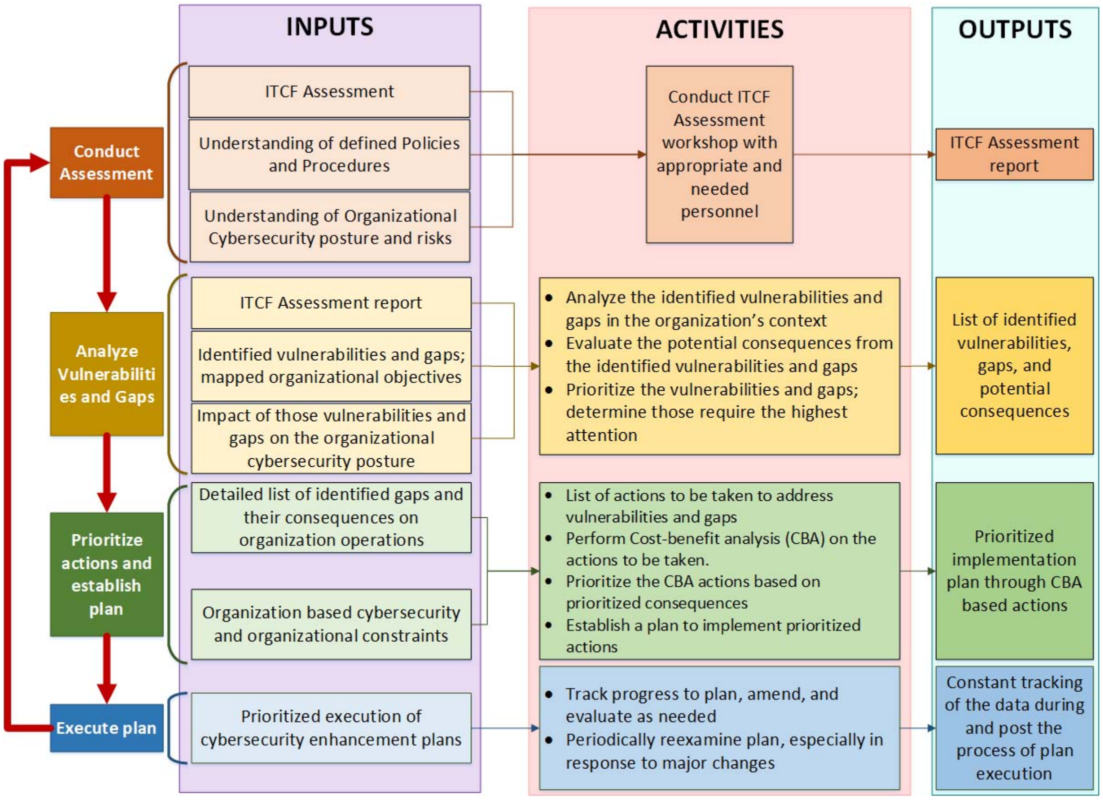
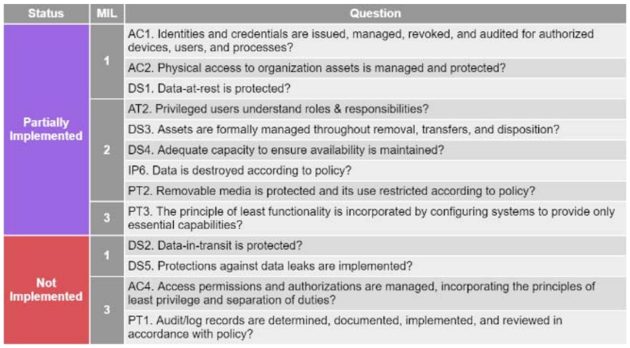

INPUTS
ACTIVITIES
OUTPUTS
Conduct Assessment
ITCF Assessment
Understanding of defined Policies and Procedures
Understanding of Organizational Cybersecurity posture and risks
Conduct ITCF Assessment workshop with appropriate and needed personnel
ITCF Assessment report
Analyze Vulnerabilities and Gaps
ITCF Assessment report
Identified vulnerabilities and gaps; mapped organizational objectives
Impact of those vulnerabilities and gaps on the organizational cybersecurity posture
Analyze the identified vulnerabilities and gaps in the organization's context
Evaluate the potential consequences from the identified vulnerabilities and gaps
Prioritize the vulnerabilities and gaps; determine those require the highest attention
List of identified vulnerabilities, gaps, and potential consequences
Prioritize actions and establish plan
Detailed list of identified gaps and their consequences on organization operations
Organization based cybersecurity and organizational constraints
List of actions to be taken to address vulnerabilities and gaps
Perform Cost-benefit analysis (CBA) on the actions to be taken.
Prioritize the CBA actions based on prioritized consequences
Establish a plan to implement prioritized actions
Prioritized implementation plan through CBA based actions
Execute plan
Prioritized execution of cybersecurity enhancement plans
Track progress to plan, amend, and evaluate as needed
Periodically reexamine plan, especially in response to major changes
Constant tracking of the data during and post the process of plan execution

Fig. 10. Recommended approach for using ITCF

TABLE I. Illustrative Gap Analysis *(Identified Gaps)* – Protect



Status	MIL	Question
Partially Implemented	1	AC1. Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes?
		AC2. Physical access to organization assets is managed and protected?
		DS1. Data-at-rest is protected?
	2	AT2. Privileged users understand roles & responsibilities?
		DS3. Assets are formally managed throughout removal, transfers, and disposition?
		DS4. Adequate capacity to ensure availability is maintained?
		IP6. Data is destroyed according to policy?
		PT2. Removable media is protected and its use restricted according to policy?
	3	PT3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities?
Not Implemented	1	DS2. Data-in-transit is protected?
		DS5. Protections against data leaks are implemented?
	3	AC4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties?
		PT1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy?

A. Case-Study – 1

Based on the review of several insider attacks, we identified that a number of key patterns and security gaps were exploited: 1) Trusted staff members have administrative access, but their usage is not carefully monitored and logged; 2) Minimal/ no access control for employees with access to sensitive data; 3) Minimal/no monitoring and restrictive measures in the areas where employees can share sensitive information; 4) Administrator privileges are not verified when changed and/or elevated; 5) Lack of asset classification and inventory management; 6) Lack of audit and review of system configurations; 7) Employee privileges and access controls are not updated as needed based on "requirement to access;" 8) Physical security measures are strictly implemented including strong procedures to access restricted areas; 9) Cyber and physical security monitoring systems are not properly implemented; 10) Technical controls such as least privilege system, entitlement management system, and asset classification system are partially implemented; 11) Staff reviews access logs, trained to prevent access escalation.

In addition to the security gaps noted above, the underlying nature of the organization's security posture [14] is retained for the purposes of this use case. Below are the retained aspects of the organization. To capture and illuminate key security gaps in the above use case, modifications to the fictitious organization are *italicized and underlined*:

1. As of current date, management has prioritized the organization mission, objectives, and activities. The organization's role in the supply chain and critical infrastructure are mostly identified but the details of the organization dependencies and critical functions for delivery of critical services, and organization resilience requirements to support the delivery are not established. No methods are in place to determine the risk tolerance.
2. The organization has inventoried, prioritized critical cyber assets and resources (hardware, devices, data, software).
   - Monitoring *methods are only partially implemented*.
   - Internal, external communication/Info. systems, data flow management are only partially implemented.
3. The employees are given physical access to key organizational assets and remote access to critical cyber assets based on their issued identities and credentials.
   - *Access (control) permissions are not managed by incorporating the principles of least privilege and separation of duties.*
   - *All employees are trained and they (including third-party stakeholders, privilege employees, senior executives, physical/information security personnel) are well informed of their cyber/information security roles and responsibilities (legal and regulatory).*
   - *Cybersecurity practices are strongly incorporated in Human Resources activities and a vulnerability management plan is being developed*.
4. The organization's information security policy, *including* the governance and risk management processes to address the cybersecurity risks are *well established*. Potential business impacts, likelihoods, risk responses are identified, prioritized. Asset vulnerabilities and threats (both internal and external) are mostly identified and documented, but they are not used to determine/understand risk, attack methods and impact of events on business continuity.
5. The organization's risk (or, cyber supply chain risk) management processes are established, managed, mostly agreed upon by organization stakeholders. Organization owners and operators have identified and prioritized their suppliers and partners. Their contract to meet the objectives of information security program/cyber supply chain risk management plan is still in progress. The evaluations of suppliers/providers are not yet conducted.
6. Protections against data leaks (data-at-rest and data-in-transit) are *moderately implemented*. Integrity checking mechanisms to verify integrity of critical cyber assets, organization automation and energy management/ technology systems are not put into practice yet. Assets are mostly managed throughout removal, transfers and disposition and adequate capacity is partially supported. *The development and testing environment(s) are separate from the production environment*.
7. Maintenance and repair of organizational assets are performed and logged in a timely manner, but their remote maintenance has not been approved. Audit/log records are partially documented. Removable media and organization IT and OT networks are protected in certain areas of the organization. Systems operate in pre-defined functional states but have not been configured to incorporate the principle of least functionality. Backups of information are conducted and tested periodically. The organization *has* a baseline configuration of organization information technology, system development life cycle, configuration change control processes, and policy & regulations regarding the physical operating environment. *All data is retained, and no strong data destruction policies are implemented*. Protection and detection processes are tested *and updated except for some of the access control policies*.
8. Incident alert thresholds are *partially established*. Event data is mostly aggregated and correlated from multiple sources and sensors. Detection roles and responsibilities are *partially defined*. Detection activities partially comply with all applicable requirements.
9. The network, physical environment and personnel activity to detect potential cybersecurity events are *monitored occasionally. The system is constantly updated to detect malicious code and periodic vulnerability scans are performed. The system monitors for unauthorized personnel, connections, devices and software. Therefore, unauthorized mobile code is strictly detected*.
10. Response and recovery planning documents are up to date. Response and recovery plans would be executed/ implemented during an event. Personnel knows their roles and order of operations when a response is needed. But the events are not reported consistently with an established response plan. Information is partially shared; Voluntary information sharing and coordination with stakeholders mostly occurs with a response plan to achieve broader cybersecurity situational awareness. Notification from detection systems are investigated; *forensics are performed*; *incidents are expected to be contained*, mitigated and categorized with response plans; *newly identified vulnerabilities are documented*. Response plan and recovery strategies are updated periodically. Response and Recovery plans mostly contain lessons learned. *Recovery activities are communicated to stakeholders and management teams. Protocols required for post-event reputation repair are established*.

B. ITCF Evaluation: Results

The illustrative responses above are illuminated as ITCF questions are answered by various organization staff. The ITCF webtool is used to answer a total of 100+ questions covering various aspects discussed in previous sections. It is evident from Fig. 11 and Table II-VI that the organization has gaps. Management can use this analysis to prioritize strategic investments to address improving those areas identified as *Partially Implemented* and *Not Implemented.*

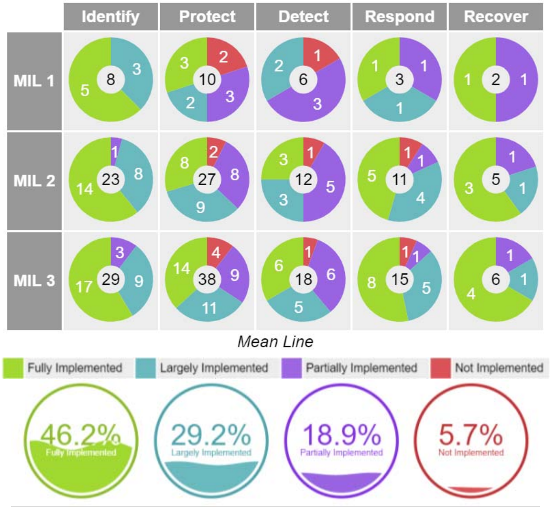
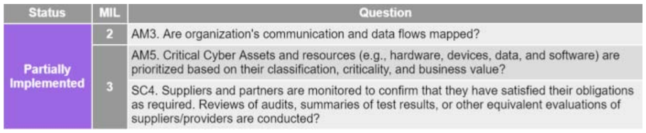


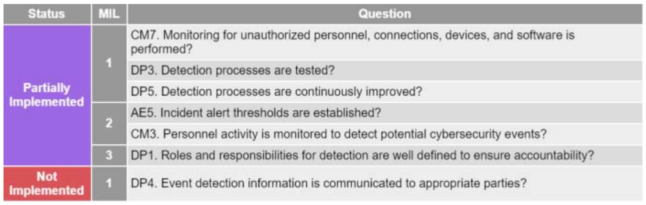
Fig. 11. Summary of the organization's cybersecurity posture and gaps

TABLE II. GAP ANALYSIS *(IDENTIFIED GAPS)* – IDENTIFY



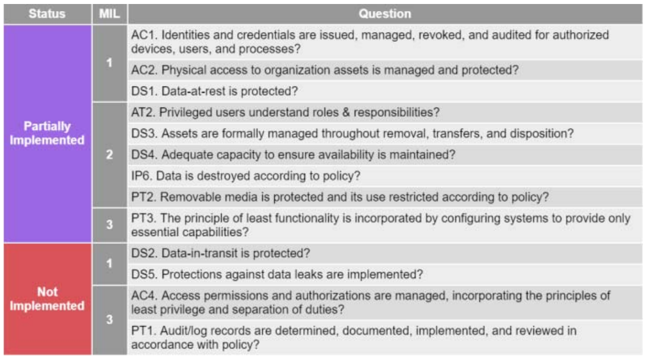
Status	MIL	Question
Partially Implemented	2	AM3. Are organization's communication and data flows mapped?
	3	AM5. Critical Cyber Assets and resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value?
		SC4. Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted?

TABLE III. GAP ANALYSIS *(IDENTIFIED GAPS)* – DETECT



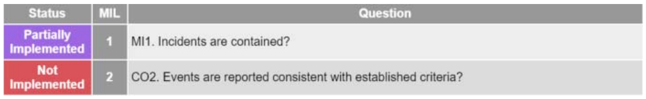
Status	MIL	Question
Partially Implemented	1	CM7. Monitoring for unauthorized personnel, connections, devices, and software is performed?
		DP3. Detection processes are tested?
		DP5. Detection processes are continuously improved?
	2	AE5. Incident alert thresholds are established?
		CM3. Personnel activity is monitored to detect potential cybersecurity events?
	3	DP1. Roles and responsibilities for detection are well defined to ensure accountability?
Not Implemented	1	DP4. Event detection information is communicated to appropriate parties?

TABLE IV. GAP ANALYSIS *(IDENTIFIED GAPS)* – PROTECT



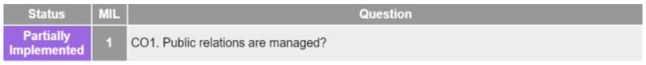
Status	MIL	Question
Partially Implemented	1	AC1. Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes?
		AC2. Physical access to organization assets is managed and protected?
		DS1. Data-at-rest is protected?
	2	AT2. Privileged users understand roles & responsibilities?
		DS3. Assets are formally managed throughout removal, transfers, and disposition?
		DS4. Adequate capacity to ensure availability is maintained?
		IP6. Data is destroyed according to policy?
		PT2. Removable media is protected and its use restricted according to policy?
	3	PT3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities?
Not Implemented	1	DS2. Data-in-transit is protected?
		DS5. Protections against data leaks are implemented?
	3	AC4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties?
		PT1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy?

TABLE V. GAP ANALYSIS *(IDENTIFIED GAPS)* – RESPOND



Status	MIL	Question
Partially Implemented	1	MI1. Incidents are contained?
Not Implemented	2	CO2. Events are reported consistent with established criteria?

TABLE VI. GAP ANALYSIS *(IDENTIFIED GAPS)* – RECOVER



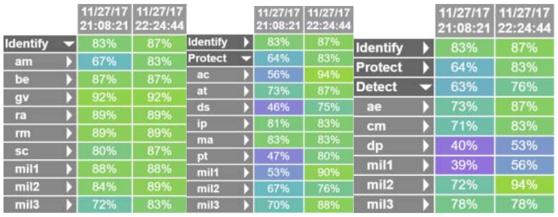
Status	MIL	Question
Partially Implemented	1	CO1. Public relations are managed?

C. Post Investment Cybersecurity Assessment

1. Investments are made to prioritize critical cyber assets based on their classification, criticality, and business value. Although this has not been fully achieved, it is largely achieved throughout the organization. All the organization's communication and data flows are mapped.
2. The organization has had high reputation in their ability to monitor suppliers and partners regarding their obligations towards the organization. But, in the past, audits were not conducted periodically. Investments are directed towards ensuring this gap is mitigated.
3. Strong focus towards ensuring the enforcement of strong protection systems in the organization: A) Asset access management is strictly monitored and managed through multiple layers of authorities; B) Periodic credential management systems are implemented; C) Permissions are managed through least privilege and separation of duties principles; D) Periodic training platforms and sessions are established to train the privileged users about their roles and responsibilities. Random periodic security checks are implemented to ensure the integrity of the employees; E) Large investments are directed towards achieving high data security. Some principles focusing data-at-rest and data-in-transit protection are prioritized. Protection against data leaks has been highly prioritized and fully implemented. Other areas are work-in-progress; F) although data destruction is not acceptable at the organizational level, data containment methods have been enhanced with strict monitoring systems around the storage locations/systems; G) New rules have been imposed to ensure periodic reviews of audit/log records. Absolute prohibition of the use of removable media has been implemented in critical areas of the organization; H) Currently, work is in progress to fully implement the principle of least functionality by configuring systems to provide only essential capabilities.
4. The organization improved their detection systems and mechanisms as the next on the prioritized list of actions: A) A new team has been set in motion to ensure constant micro-monitoring. All personnel activity is monitored. Incident alert thresholds are established; B) Currently, the organization is rigorously focusing on improving the roles and responsibilities for detection and the tests associated with detection processes; C) Rules are set in motion to improve communication processes about event detection.
5. Event reporting rules and related criteria are established. Mechanisms to contain the incidents are set in motion but are not fully implemented. Methods to manage public relations are improved and established across several sections in the organization.

D. Pre-investment vs Post-investment

Pre- and post-investment cybersecurity assessments are compared using ITCF's built-in comparative analysis plugin. These comparative analyses are shown in figures below.

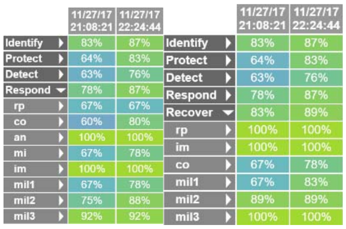


	11/27/17 21:08:21	11/27/17 22:24:44
Identify	83%	87%
am	67%	83%
be	87%	87%
gv	92%	92%
ra	89%	89%
rm	89%	89%
sc	80%	87%
mil1	88%	88%
mil2	84%	89%
mil3	72%	83%

	11/27/17 21:08:21	11/27/17 22:24:44
Identify	83%	87%
Protect	64%	83%
ac	56%	94%
at	73%	87%
ds	46%	75%
ip	81%	83%
ma	83%	83%
pt	47%	80%
mil1	53%	90%
mil2	67%	76%
mil3	70%	88%

	11/27/17 21:08:21	11/27/17 22:24:44
Identify	83%	87%
Protect	64%	83%
Detect	63%	76%
ae	73%	87%
cm	71%	83%
dp	40%	53%
mil1	39%	56%
mil2	72%	94%
mil3	78%	78%

Fig. 12. Improvement in Cybersecurity posture in *Identify, Protect, Detect*



	11/27/17 21:08:21	11/27/17 22:24:44
Identify	83%	87%
Protect	64%	83%
Detect	63%	76%
Respond	78%	87%
rp	67%	67%
co	60%	80%
an	100%	100%
mi	67%	78%
im	100%	100%
mil1	67%	78%
mil2	75%	88%
mil3	92%	92%

	11/27/17 21:08:21	11/27/17 22:24:44
Identify	83%	87%
Protect	64%	83%
Detect	63%	76%
Respond	78%	87%
Recover	83%	89%
rp	100%	100%
im	100%	100%
co	67%	78%
mil1	67%	83%
mil2	89%	89%
mil3	100%	100%

Fig. 13. Improvement in Cybersecurity posture in *Respond, Recover*

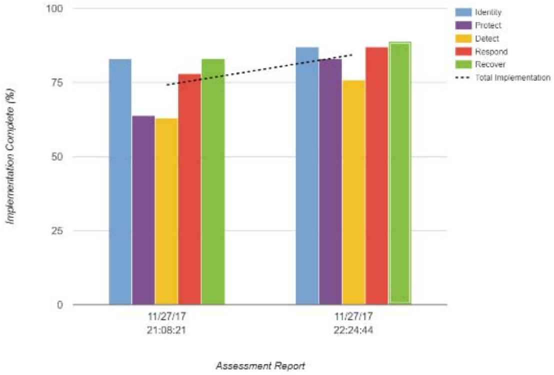


Fig. 14. Positive investment reflection across all domains

Organizations can use the above data analytics capability to estimate return on investments. Currently, our team is also developing the capability to perform these calculations and generate a summary of cost-benefit analysis.

E. Case-Study – 2

Over the last decade, there have been many highly publicized insider cyber & physical attacks against critical infrastructures. A number of these attacks included critical water infrastructure, such as treatment and distribution plants[15, 16]. Analysis of these case-studies provides valuable insight into the security defenses that are needed to prevent insider and other complex cyber-attacks.

Description of this case-study: Between March and April of 2001, a third-party utility contractor carried out an insider attack on his employers that caused over 200,000 gallons of sewage water to spill. While employed, he worked on a team to install SCADA radio-controlled sewage equipment at the water treatment plant. Towards the end of the project, he left his job over some disagreements with his employer. Even though his employment was terminated, the third-party contractor's credentials and access to the plant's critical control systems were not revoked. He still had access to these critical systems and was able to issue radio commands to disable the alarms at four pumping stations and spoof the network address. Through those exploits, he executed a cyber-attack that caused a physical impact. Forensic analysis of the attack, suggests that the third-party contractor could exploit vulnerable SCADA systems and issue malicious commands without any actionable alarms or monitoring. The utility lacked basic cybersecurity policies, procedures and systems to prevent such an attack. Notable among them, and included in the ICTF, the water treatment plant's control systems lacked basic access controls defined in NIST SP 800-53 [17]. The attack on the water utility may have been prevented if the utility had conducted an ICTF assessment and implemented even a basic level of its recommend controls found in [15, 18].

Based on the brief analysis on the incident, the illustrative organization in case-study-2 is modified to include the vulnerabilities identified in the water treatment plant. Changes to the organization posture from case-study-2 include:

- **Identify:** Asset management is partially implemented; minimal to no risk assessment principles are in place – lack of documented threats and vulnerabilities; the organization has minimal monitoring methods of the partners
- **Protect:** Access control management is poorly implemented. There are critical gaps in managing remote access, lack of network segregation; employees are trained periodically; data security measures are implemented; does not have strong configuration management systems; remote maintenance measures are not up-to-date
- **Detect:** Continuous monitoring measures are partially implemented; detection processes are poorly implemented, and they are not updated periodically.
- **Respond:** Overall, the organization has well-defined response plans, but it lacks forensic methods, incident containment and mitigation measures**.**
- **Recover:** All processes are up-to-date – no gaps are found.

F. ITCF Evaluation: Results

An ICTF assessment is performed for the above fictitious organization that may emulate the cybersecurity posture of the water treatment plant.

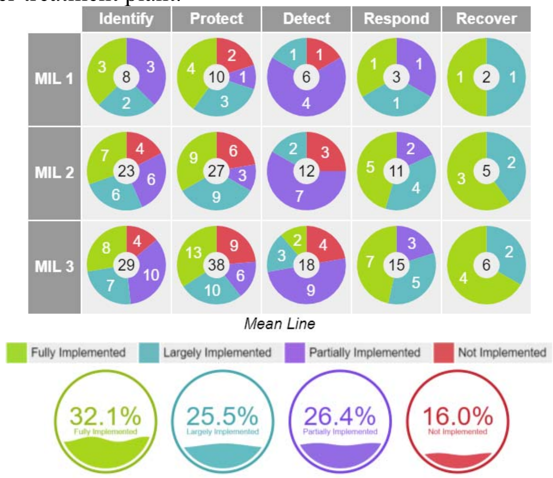
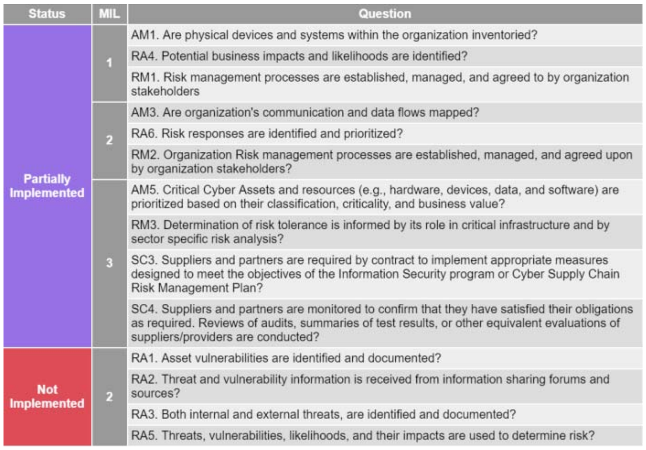


Fig. 15. Summary of the organization's cybersecurity posture and gaps

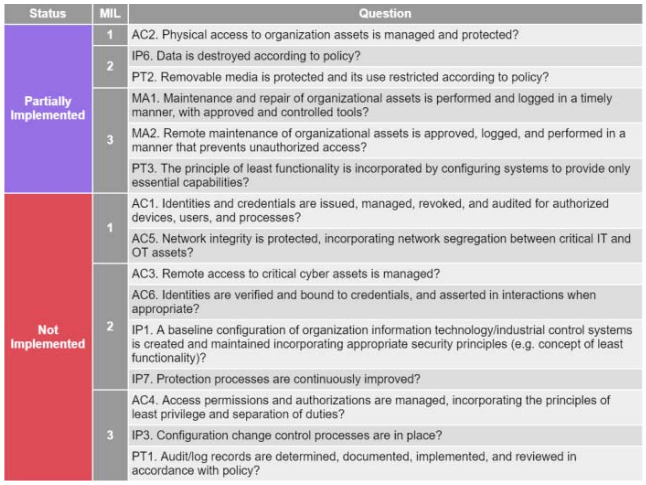
It is evident that the organization has gaps and those gaps are further detailed in Fig. 15 and in Table-VII – XI. The organization's management could decide the path to direct their investments towards turning some of the partially implemented and not implemented areas to largely implemented or fully implemented.

TABLE VII. GAP ANALYSIS *(IDENTIFIED GAPS)* – IDENTIFY



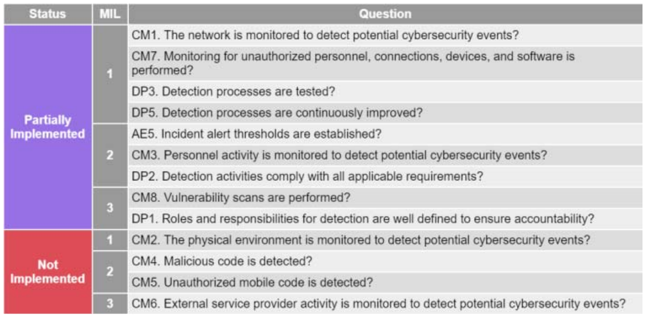
Status	MIL	Question
Partially Implemented	1	AM1. Are physical devices and systems within the organization inventoried?
		RA4. Potential business impacts and likelihoods are identified?
		RM1. Risk management processes are established, managed, and agreed to by organization stakeholders
	2	AM3. Are organization's communication and data flows mapped?
		RA6. Risk responses are identified and prioritized?
		RM2. Organization Risk management processes are established, managed, and agreed upon by organization stakeholders?
	3	AM5. Critical Cyber Assets and resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value?
		RM3. Determination of risk tolerance is informed by its role in critical infrastructure and by sector specific risk analysis?
		SC3. Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan?
		SC4. Suppliers and partners are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of suppliers/providers are conducted?
Not Implemented	2	RA1. Asset vulnerabilities are identified and documented?
		RA2. Threat and vulnerability information is received from information sharing forums and sources?
		RA3. Both internal and external threats, are identified and documented?
		RA5. Threats, vulnerabilities, likelihoods, and their impacts are used to determine risk?

TABLE VIII. GAP ANALYSIS *(IDENTIFIED GAPS)* – PROTECT



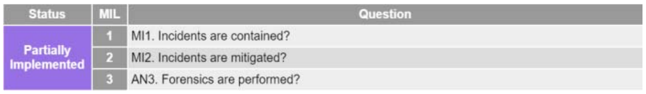
Status	MIL	Question
Partially Implemented	1	AC2. Physical access to organization assets is managed and protected?
	2	IP6. Data is destroyed according to policy?
		PT2. Removable media is protected and its use restricted according to policy?
	3	MA1. Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools?
		MA2. Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access?
		PT3. The principle of least functionality is incorporated by configuring systems to provide only essential capabilities?
Not Implemented	1	AC1. Identities and credentials are issued, managed, revoked, and audited for authorized devices, users, and processes?
		AC5. Network integrity is protected, incorporating network segregation between critical IT and OT assets?
	2	AC3. Remote access to critical cyber assets is managed?
		AC6. Identities are verified and bound to credentials, and asserted in interactions when appropriate?
		IP1. A baseline configuration of organization information technology/industrial control systems is created and maintained incorporating appropriate security principles (e.g. concept of least functionality)?
		IP7. Protection processes are continuously improved?
	3	AC4. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties?
		IP3. Configuration change control processes are in place?
		PT1. Audit/log records are determined, documented, implemented, and reviewed in accordance with policy?

TABLE IX. GAP ANALYSIS *(IDENTIFIED GAPS)* – DETECT



Status	MIL	Question
Partially Implemented	1	CM1. The network is monitored to detect potential cybersecurity events?
		CM7. Monitoring for unauthorized personnel, connections, devices, and software is performed?
		DP3. Detection processes are tested?
		DP5. Detection processes are continuously improved?
	2	AE5. Incident alert thresholds are established?
		CM3. Personnel activity is monitored to detect potential cybersecurity events?
		DP2. Detection activities comply with all applicable requirements?
	3	CM8. Vulnerability scans are performed?
		DP1. Roles and responsibilities for detection are well defined to ensure accountability?
Not Implemented	1	CM2. The physical environment is monitored to detect potential cybersecurity events?
	2	CM4. Malicious code is detected?
		CM5. Unauthorized mobile code is detected?
	3	CM6. External service provider activity is monitored to detect potential cybersecurity events?

TABLE X. GAP ANALYSIS (IDENTIFIED GAPS) – RESPOND



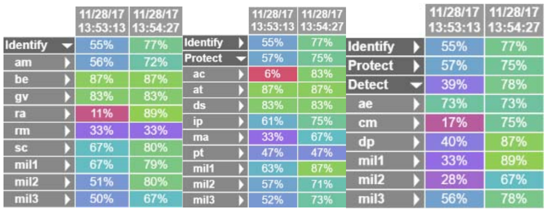
Status	MIL	Question
Partially Implemented	1	MI1. Incidents are contained?
	2	MI2. Incidents are mitigated?
	3	AN3. Forensics are performed?

G. Post Investment Cybersecurity Assessment

- **Identify:** A team is set in motion to inventory, manage all the assets, to identify associated threats, vulnerabilities and risks; monitoring methods are implemented over partners.
- **Protect:** As the organization identified that the lack of strong access control was the biggest security gap, large investments are directed towards improving these mechanisms; next, the organization focused on improving the configuration management methods; maintenance procedures are now updated periodically and as needed
- **Detect:** Physical, network, personnel monitoring systems are implemented; roles and responsibilities and detection processes are implemented and updated periodically;
- **Respond:** Incident containment, mitigation methods are highly improved; the organization's next goal is to improve forensics but not implemented at current state.

H. Pre-investment vs Post-investment

Pre- and post-investment cybersecurity assessments are compared using ITCF's built-in comparative analysis plugin. These comparative analyses are shown in figures below.

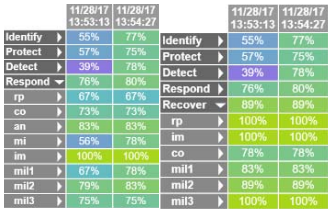


	11/28/17 13:53:13	11/28/17 13:54:27
Identify	55%	77%
am	56%	72%
be	87%	87%
gv	83%	83%
ra	11%	89%
rm	33%	33%
sc	67%	80%
mil1	67%	79%
mil2	51%	80%
mil3	50%	67%

	11/28/17 13:53:13	11/28/17 13:54:27
Identify	55%	77%
Protect	57%	75%
ac	6%	83%
at	87%	87%
ds	83%	83%
ip	61%	75%
ma	33%	67%
pt	47%	47%
mil1	63%	87%
mil2	57%	71%
mil3	52%	73%

	11/28/17 13:53:13	11/28/17 13:54:27
Identify	55%	77%
Protect	57%	75%
Detect	39%	78%
ae	73%	73%
cm	17%	75%
dp	40%	87%
mil1	33%	89%
mil2	28%	67%
mil3	56%	78%

Fig. 16. Improvement in Cybersecurity posture in *Identify, Protect, Detect*



	11/28/17 13:53:13	11/28/17 13:54:27
Identify	55%	77%
Protect	57%	75%
Detect	39%	78%
Respond	76%	80%
rp	67%	67%
co	73%	73%
an	83%	83%
mi	56%	78%
im	100%	100%
mil1	67%	78%
mil2	79%	83%
mil3	75%	75%

	11/28/17 13:53:13	11/28/17 13:54:27
Identify	55%	77%
Protect	57%	75%
Detect	39%	78%
Respond	76%	80%
Recover	89%	89%
rp	100%	100%
im	100%	100%
co	78%	78%
mil1	83%	83%
mil2	89%	89%
mil3	100%	100%

Fig. 17. Improvement in Cybersecurity posture in *Respond, Recover*

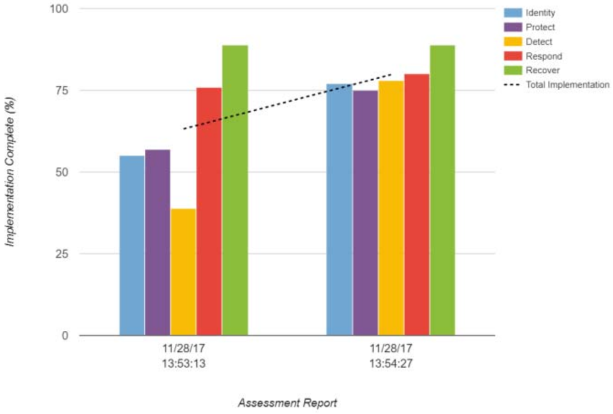


Fig. 18. Positive investment reflection across all domains

V. Conclusion

Insider cyber-physical threats will continue to be a major challenge for organizations. The case studies of insider cyber-attacks suggest that organizations with mature, proactive insider threat programs are better positioned to identify, deter, detect, and mitigate insider threats before they are able to cause serious harm [19].

This paper helped validate and verify the effectiveness of the Insider Threat Cybersecurity Framework (ITCF) webtool and methodology can help defend against these complex, non-linear and evolving cyber-physical threats. Applying ITCF to two case-studies further demonstrated the efficacy of ITCF's approach to combating insider cyber-physical threats and realizing cybersecurity risk management goals for critical infrastructure organizations. Effective cybersecurity is often not a single solution, but a continuous process that requires a holistic, agile approach. ITCF provides a webtool, methodology and various features to help organizations realize their cybersecurity goals and combat cyber-physical insider threats. ICTF features include but are not limited to: an easy-to-use rapid assessment tool to perform an insider threat self-assessment; determines the current insider threat cybersecurity posture; defines investment-based goals to achieve a target state; and, finally, connects the cybersecurity posture with business processes, functions, and continuity.

The ITCF also comprehensively addresses technical indicators of insider threat and cybersecurity risk in accordance with NIST guidance and federal legislation. Robust insider threat programs require collaboration between and among many disparate information sources. Future research will be focused on expansion of the Identify, Protect, Defend, Respond and Recover domains to include additional organizational factors which can contribute to a comprehensive risk management strategy. Organizational factors such as task difficulty, time and budget constraints, and lack of career advancements [20] are identified as key contributors to actions perpetrated by a malicious or unintentional insider. These workplace characteristics influence a variety of things including employee morale, job satisfaction, and safety culture. The integration of human factors into the ITCF will provide an improved tool for organizations to leverage when developing a defense-in-depth security posture against insider and other complex cyber-physical threats. As showed, an advantage of ITCF over other existing frameworks [21] is that the ITCF follows NIST cybersecurity framework to meet EO 13800, addresses both policy level and systems level cybersecurity challenges, and provides an easy-to-use interactive webtool. Future work would focus on performing ITCF assessments on real facilities that may lead to the development of further case studies that focuses on specific organizational type. Lessons learned from those assessment as well as other existing frameworks [21] will be used to further improve the ITCF webtool.

References

[1] Executive Order 13587: Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 2012

[2] Obama, B. National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, 2012.

[3] M. G. Gelles, 'Insider Threat: Prevention, Detection, Mitigation, and Deterrence', Elsevier Science, 2016.

[4] G. Silowash, D. Cappelli, et al.,'Common sense guide to mitigating insider threats 4th edition', Software Engineering Institute, 2012.

[5] Dtex Systems, 'New Study Reveals Costly Effects of Insider Threats on the Enterprise, Underscores Gap in Legacy Solutions'. https://dtexsystems.com/new-study-reveals-costly-effects-of-insider-threats-on-the-enterprise-underscores-gap-in-legacy-solutions/, 2017.

[6] O. Brdiczka, 'Insider Threats - the myth of the black swan'. https://www.computerworld.com/article/2839063/security0/insider-threats-the-myth-of-the-black-swan.html, accessed Nov. 28, 2017.

[7] 'National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs', https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf/ncsc-nittf-policy-legal, accessed Nov. 28, 2017.

[8] S. Amin, et al., 'In quest of benchmarking security risks to cyber-physical systems', IEEE Network, 2013, 27, (1), pp. 19-24.

[9] 'Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure'. https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal, accessed Nov. 29, 2017.

[10] 'Framework for Improving Critical Infrastructure Cybersecurity'. https://www.nist.gov/cyberframework/draft-version-11

[11] J. Haggerman, M. Mylrea, S. Gourisetti, A. Nicholls, 'Organizations Cybersecurity Framework'. PNNL-EERE, (Forthcoming), 2017.

[12] M. Mylrea, S. Gourisetti, A. Nicholls, 'An Introduction to Organizations Cybersecurity Framework'. Proc. IEEE Symposium on Computational Intelligence Applications in Smart Grid, Hawaii, 2017.

[13] T. Sommestad, M. Ekstedt, P. Johnson, 'Cyber security risks assessment with bayesian defense graphs and architectural models'. 42nd Hawaii International Conference on System Sciences, 2009 pp. 1-10.

[14] S. Gourisetti, et al., 'Multi-Scenario Use Case based Demonstration of Buildings Cybersecurity Framework Webtool'. IEEE Symposium on Computational Intelligence Applications in Smart Grid, Hawaii, 2017.

[15] M. Abrams, and J. Weiss, 'Malicious control system cyber security attack case study–Maroochy Water Services, Australia', McLean, VA: The MITRE Corporation, 2008

[16] L. J. Van Leuven, 'Water/wastewater infrastructure security: threats and vulnerabilities': 'Handbook of water and wastewater systems protection', Springer, 2011, pp. 27-46

[17] R. S. Ross, 'Security and Privacy Controls for Federal Information Systems and Organizations', (NIST SP)-800-53 Rev 4, 2013

[18] NIST 800-53 Compliance Solutions: Compliance Automation and Self-service Administration'. https://www.avatier.com/solutions/governance-risk-and-compliance/fisma/nist-800-53/, accessed 2017.

[19] National Insider Threat Task Force. '2017 Insider Threat Guide" A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards,' 2017. https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf

[20] F. Greitzer, M. Imran, et.al. 'Developing an Ontology for Individual and Organizational Sociotechnical Indicators of Insider Threat Risk.' Semantic Technology for Intelligence, Defense, and Security (STIDS), 2016. Available at: http://stids.c4i.gmu.edu/papers/STIDSPapers/STIDS 2016_T03 _GreitzerEtAl.pdf

[21] EY, "Managing Insider Threat: A holistic approach to dealing with risk from within", 2016. Available at: http://www.ey.com/Publication/vwLUAssets/EY-managing-insider-threat-a-holistic-approach-to-dealing-with-risk-from-within/$FILE/EY-managing-insider-threat.pdf

Appendix

Below are a representative sample of questions from the ITCF in the Protect domain.

MIL1:

Are identities and credentials issued, managed, revoked, and audited for authorized devices, users, and processes?

Is Physical access to organization assets managed and protected?

Is data-at-rest protected?

Is data-in-transit protected?

Are protections against data leaks implemented?

MIL2:

Do priveliged users understand roles and responsibilities?

Are assets formally managed throughout removal, transfers, and disposition?

Is there adequate capacity to ensure availability is maintained?

MIL3:

Is the principle of least functionality incorporated by configuring systems to provide only essential capabilities?

Are access permissions and authorizations managed, incorporating the principles of least privilege and separation of duties?

Are audit/log records determined, documented, implemented, and reviewed in accordance with policy?