Information Technology Sector

Risk Management Strategy for the *Provide Incident Management Capabilities* Critical Function

July 2011

Contents

Figures

Table

Executive Summary

Public and private owners and operators completed the first ever functions-based IT Sector Baseline Risk Assessment in August 2009. This assessment describes risks from manmade deliberate, manmade unintentional and natural threats to producers and providers of IT hardware, software and services using threat, vulnerability, and consequence frameworks. The ITSRA resulted in an IT Sector Risk Profile that identifies national-level risks of concern for the IT Sector. Public and private sector partners collaboratively developed the assessment, which reflects the expertise of participating subject-matter experts (SME).

Critical IT Sector Functions

- *Provide IT products and services*
- ***Provide incident management capabilities***
- *Provide domain name resolution services*
- *Provide identity management and associated trust support services*
- *Provide Internet-based content, information, and communications services*
- *Provide Internet routing, access, and connection services*

Using the risks identified in the ITSRA, IT Sector partners are systematically addressing the risks of concern for each critical function by engaging in risk management analyses, and where necessary, they will also define and propose mitigation strategies to reduce national level risks.

Within the risk management analyses, SMEs are assessing the merits and drawbacks of taking one of four approaches to risk mitigation:

- **Risk Avoidance** involves methods to decrease the likelihood of occurrence by removing a hazard or ending a specific exposure.
- **Risk Acceptance** refers to dealing with a risk when or after it occurs. If the cost of mitigating a risk is greater than the potential loss, accepting the risk may be the most viable strategy.
- **Risk Mitigation** involves methods that reduce the severity of the loss or decrease the likelihood of the loss from occurring.
- **Risk Transfer** can be best described as a shifting of risk from one entity to another. When a risk occurs, the losses are absorbed by another entity.

Potential risk responses include a wide array of possible solutions and may involve accepting less likely and less consequential risks, improving physical security, establishing logical, electronic, or cyber access controls, or neutralizing threats before they can be launched against physical and cyber infrastructure assets. Identifying risk responses and prioritizing the mitigations for identified IT Sector risks helps ensure that resources are applied where they can most effectively respond to the threats, vulnerabilities, and/or consequences facing the critical IT Sector functions.

The objective of the sector's risk response and prioritization methodology is to achieve the greatest overall risk reduction by selecting the most effective risk response to functions that would have the greatest impact on sector capabilities. Beginning with the high-priority risks of concern, each ITSRA-identified risk is evaluated to determine the most feasible and effective management response to the respective risk. To determine the effectiveness of a potential risk response, IT Sector SMEs estimate the level to which each risk is most likely to be reduced.

The combination of the estimated effectiveness and estimated feasibility factors for each potential risk response are evaluated to determine which risk response is most appropriate. Often, a risk response that offers the highest risk reduction may not present the most appropriate response for the IT Sector because it may not be feasible. Thus, a less effective risk response with a higher feasibility may present the best option.

This approach guides the decision making process of selecting a risk response by explicitly linking each risk to a potential response, allowing sector partners to prioritize the risks identified in the ITSRA and identify the most effective method(s) of mitigating those risks.

Once the appropriate risk response is identified for a specific risk of concern to a function, Sector partners determine if implementing this response would (positively or negatively) impact the overall sector risk profile or if it impacts other critical IT Sector functions' risk profiles. If the Sector partners determine that implementation of the respective risk response does not adversely affect other functions' risk profiles or that of the overall sector, then the risk response is implemented. If it is determined that a risk response would negatively impact the sector or functions' risk profiles, then an alternative risk response approach will be identified.

Where mitigation is the preferred risk response, IT Sector partners identify appropriate Risk Mitigation Activities (RMA) to reduce national-level risks across each critical function based on SME input. The identified risk responses and the prioritization of the mitigations for identified IT Sector risks will inform resource allocation to most effectively respond to the threats, vulnerabilities, and/or consequences facing the critical IT Sector functions. IT Sector partners analyzed the ITSRA risks of concern to the *Provide Incident Management Capabilities* critical function and developed mitigation responses to three risks of concern. The risks, associated RMAs, and resulting likelihood and consequence ratings appear in Table 1.

Table 1: Risk and Mitigation Overview

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings[1]
Lack of Data: Impact to Detection	Medium likelihood; Medium consequence	• Duplicate geographically distinct storage areas • Move toward federated model so that incident management is executed by multiple entities and not only by the same entity impacted • Work virtually and promote remote work environments • Disperse response capabilities • Distribute sources and content (develop a few databases of primary source data in geographically disperse areas) • Improve the way to move data (how to move data between dispersed databases and response personnel) • Clearly define the roles of the private sector and the Federal Government in responding to Significant Cyber Incidents	Low likelihood; Medium consequence
Reports Containing False	Medium likelihood;	• Conduct distribution/integrity check on data (finding multiple primary sources) • Educate workforce to recognize falsified	Low likelihood; Medium

1 Assumes complete implementation of the items noted in the Risk Mitigation Activities column

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings[1]
Information on a Vulnerability or Export: Impact to Detection	Medium consequence	information and to validate sources (training and awareness) • Vet existing reports to screen out false reports	consequence
Incident Response Prevented or Rendered Ineffective in a Timely Manner: Impact to Response	Low likelihood; Medium consequence	• Enhance training and awareness surrounding the capture of information to develop lessons learned for producers and providers of hardware and software services • Invest in or develop alternative incident management infrastructure and resources in case primaries are unavailable • Distribute response resources so they are not all negatively impacted by the same incident • Build additional redundancies into current incident management infrastructure and resources	Low likelihood; Low consequence

The final risk management strategies will inform IT Sector critical infrastructure activities, and the key elements of these strategies will be conveyed in an upcoming IT Sector Annual Report (SAR), which is the primary way in which Critical Infrastructure and Key Resources (CIKR) sector efforts and priorities are captured in support of the National Infrastructure Protection Plan (NIPP). IT Sector cybersecurity R&D requirements will be identified in the SAR and serve as inputs into the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) processes for identifying and addressing Sector needs. The report will influence cross-sector cybersecurity R&D needs and requirements and recommendations made with regard to those areas where the U.S. Government should make focused investments. In addition, the IT Sector maintains an active relationship with the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), so the IT Sector will use the results and recommendations to inform the CSIA IWG of R&D requirements. IT Sector partners will also promote the concepts of this strategy in industry and government forums to advance the risk management initiatives of the sector, and to increase the resilience of the IT Sector infrastructure.

1 Information Technology Sector Risk Management Overview

The National Infrastructure Protection Plan (NIPP), initially developed and published in 2006 and revised in 2009, specifically assigned the Department of Homeland Security (DHS) the mission of establishing uniform policies, approaches, guidelines, and methodologies for integrating infrastructure protection and risk management activities within and across CIKR sectors, along with developing metrics and criteria for related programs and activities. Using the NIPP and the IT Sector-Specific Plan (SSP), the IT Sector has been able to provide a consistent, unifying structure for integrating existing and future critical infrastructure protection and resilience efforts.

Partnership and collaboration between the IT Sector Coordinating Council (SCC) and the Government Coordinating Council (GCC) enabled the Sector to leverage their unique capabilities to address the complex challenges of CIKR protection providing both products and services that support the efficient operation of today's global information-based society.

The IT Sector uses a functions-based approach to assess and manage risks to its six critical functions. The functions-based approach promotes the assurance and resiliency of the IT infrastructure and described cascading consequences based on the Sector's interconnectedness and the critical functions' interdependencies. IT SCC and GCC partners determined that this approach would be effective for the highly distributed infrastructure that enables entities to produce and provide IT hardware, software, and services. The top-down approach enables public and private IT Sector partners to prioritize additional mitigations and protective measures to risks of national concern.

The baseline IT Sector Risk Assessment (ITSRA), released in 2009, serves as the foundation for the Sector's national-level risk management activities.[2] Public and private sector partners collaborated to conduct the assessment, which reflects the expertise and collective consensus of participating subject matter experts (SMEs). The ITSRA methodology assesses risks from manmade deliberate, manmade unintentional and natural threats that could affect the ability of the Sector's critical functions and sub-functions to support the economy and national security. The methodology leverages existing risk-related definitions, frameworks, and taxonomies from a variety of sources, including public and private IT Sector partners, standards development organizations, and policy guidance entities. By leveraging these frameworks, the IT Sector's methodology reflects current knowledge about risk and adapts them in a way that enables a functions-based risk assessment.

2 The ITSRA is available at the following URL:
http://www.it-scc.org/documents/itscc/IT_Sector_Risk_Assessment_Report_Final.pdf

2 Risk Overview – *Provide Incident Management Capabilities* Critical Function

Provide Incident Management Capabilities Function Summary	
Situation	Threats to the *Provide Incident Management Capabilities* function are varied and typically occur in parallel to incidents affecting other elements or functions of the IT infrastructure. Depending upon their severity, these incidents have the potential to deny or degrade the Sector's ability to detect, respond to, or recover from an incident.
Concern	Incidents that degrade the incident management function could have a significant aggravating effect. This effect could increase the consequences of broader incidents being managed by the IT Sector by inhibiting an effective response.
Impact	Without the ability to effectively respond to a broader incident, costs and other consequences could be significantly amplified, and recovery significantly delayed. Integrating lessons learned into future incident response procedures, policies, and prevention activities facilitates continuous improvement and fosters improved prevention and protection practices.

The IT Sector develops, provides, and operates incident management capabilities that are essential or critical to the assurance of national and economic security and public health, safety, and confidence. The *Provide Incident Management Capabilities* function includes national-level capabilities to detect, contain, resolve, and recover from incidents. Furthermore, analysis of lessons learned throughout each incident management life cycle phase enhances security partners' preparedness and prevention capabilities. The Sector's incident management capabilities are consumed by entities both internal and external to the Sector. Thus, elements of this function mitigate the overall risk to the other five IT Sector critical functions.

Supporting the incident management function are five sub-functions provided by the IT Sector. These sub-functions are:

- Provide preventive guidance, best practices, simulation, and testing;
- Provide and operate indications, alert, and warning capabilities;
- Provide and operate operation centers and teams;
- Provide and participate in information sharing, situational awareness, and information fusion activities; and
- Coordinate and provide response, recovery, and reconstitution.

The public and private sectors collectively provide the above five sub-functions. The private sector produces the majority of IT products and provides most IT services. As such, it can quickly focus on requirements and needs, and often takes the lead in developing and deploying innovative incident management solutions, increasing the skills and availability of security professionals, and developing products and services that are responsive to the rapidly changing threat environment. Public sector incident management capabilities are led by the DHS National Cybersecurity and Communications Integration Center (NCCIC). When fully mature, the NCCIC will be an integrated, 24x7 operations center that fuses internal and external cyber and communications data feeds, national intelligence, and private sector reporting into a common operating picture to enable incident response through shared situational awareness. The NCCIC coordinates inputs from private-sector entities, including the IT Information

Sharing and Analysis Center (IT-ISAC). An IT-ISAC liaison will be embedded in the NCCIC to provide real-time collaboration throughout the incident management lifecycle depicted in Figure 1.

Within the incident management lifecycle, producers and providers proactively manage risk to their own operations and those of their customers. These prevention activities are performed through constant monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions to systems, networks, and functions. Prevention efforts are advanced by using a variety of means, including the development and communication of protection strategies that organizations can implement to secure their networks and systems. Prevention and protection activities are further enhanced by IT Sector efforts to conduct operations and services that support the production of security services, such as penetration testing, risk assessments, and system testing. Although prevention and protection strategies do enhance the security of organizations, successful attacks are still possible. Therefore, to improve response and recovery operations, the IT Sector provides detection capabilities and tools so attacks against organizations' assets, systems, networks, or functions are identified as early as possible. These efforts improve response and recovery operations and overall risk management efforts. Detection is performed through a variety of means, such as technological solutions and human interaction, and it is enhanced by inter-organizational information sharing. For example, many IT Sector entities provide incident management capabilities and services, but they often do not operate independently. Instead, they cooperate and share data, through organizations such as IT-ISAC, which enhances the IT Sector's overall ability to detect and respond to malicious events. The threat information and analysis gained through this information sharing approach enables increased awareness of threats, enhancing response actions. Continued coordination between the public and private sector is needed to effectively provide incident management capabilities.

Figure 1: Incident Management Lifecycle

Response to an event includes the use of backup and recovery techniques; data retention and archiving; capacity management; and continuity of operations (COOP) plans. Like many other sectors, the IT Sector also supports response, recovery, and reconstitution through corporate social responsibility and community support activities, which occur at many levels (e.g., international, national, organization, and volunteer). In addition, the Sector provides operations centers and teams to coordinate and conduct crisis management operations.

After the Sector has responded to an incident and mitigated the consequences, it provides services that enable the recovery and reconstitution of the affected assets, systems, networks, and functions. To complete the incident management lifecycle, objective and subjective lessons learned data are recorded regarding each incident. This data serves to:

- Identify the processes, procedures, and policies that were and were not effective during the incident prevention, detection, response, and recovery stages of the incident management lifecycle.
- Update incident response policies and procedures based on successes and failures of previous incident response activities.
- Develop new prevention techniques, improving the overall incident management lifecycle for future attacks. For example:
  - Training and awareness;
  - Mechanisms to integrate incident lessons learned into subsequent product and service design and development; and
  - Improved testing procedures based on known vulnerabilities and threats.
- Improve information and intelligence flows between and across the public and private sectors to support the rapid identification of emerging cyber-related threats and other circumstances requiring intervention by government and private sector authorities.

When aggregated and used to inform future Sector-wide activities, lessons learned support the implementation of risk-based, information-driven prevention, response, and consequence management programs.

Incident Management Attack Tree and Risk Profile

Risk assessment SMEs used the incident management lifecycle approach to develop a *Provide Incident Management Capabilities* attack tree and assess undesired consequences, vulnerabilities, and threats to the incident management function. Figure 2 depicts the attack tree that scopes the baseline assessment. The attack tree focuses on three undesired consequences that could cause adverse effects on incident management at the national level:

- Impact to detection;
- Impact to response;
- Impact to recovery;
- Exploitation of recovery capabilities; and
- Impact to mitigation and prevention of similar/same attack occurrence.

Because of the wide range of vulnerabilities within the *Provide Incident Management Capabilities* function, SMEs examined manmade deliberate, manmade unintentional and natural threats to categorize possible methods by which a consequence could occur.

Figure 2: Provide Incident Management Capabilities Attack Tree (Summary)

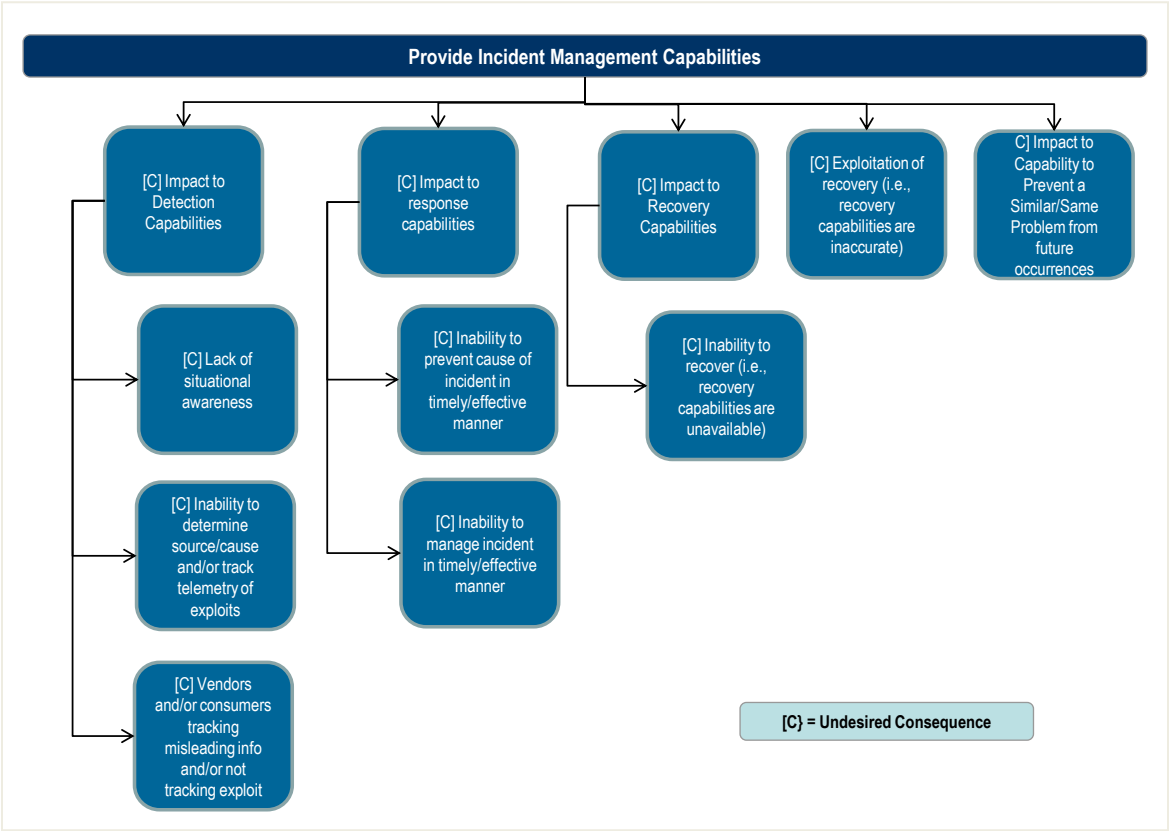
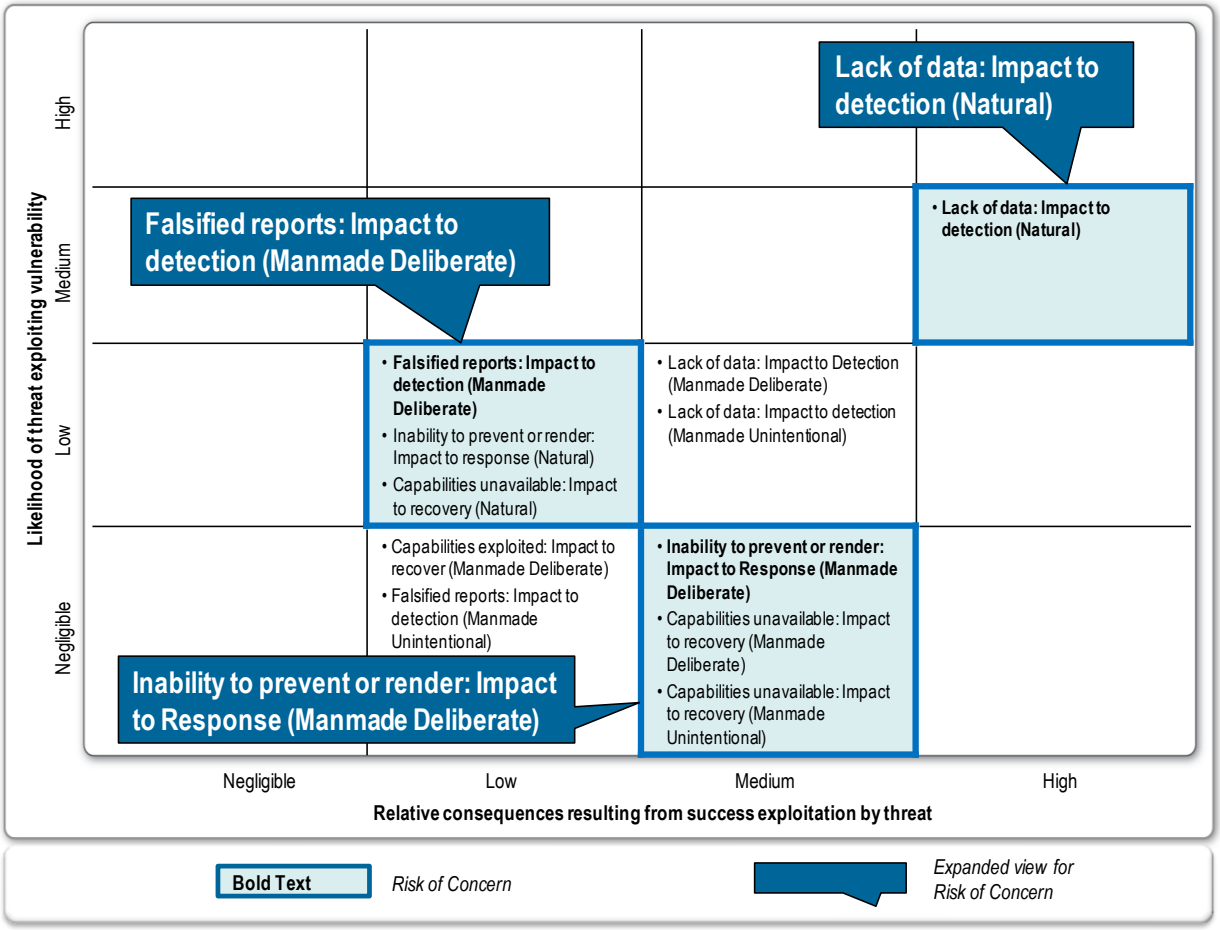


Figure 3 shows the risk profile for the *Provide Incident Management Capabilities* critical function that was developed as part of the 2009 ITSRA. This matrix maps the likelihood of a threat exploiting a vulnerability (Y-axis) against the relative consequences as a result of that threat successfully exploiting a vulnerability (X-axis).

Figure 3: Provide Incident Management Capabilities Relative Risk Table



Threats to the *Provide Incident Management Capabilities* function are varied and typically occur in parallel to attacks on other elements or functions of the IT infrastructure (i.e., incident management capabilities are not the sole target of most attacks). Depending upon their severity, incidents affecting IT Sector critical functions have the potential to deny or degrade the Sector's ability to detect, respond to, or recover from an incident. These incidents may have an aggravating effect, increasing the scale or scope of consequences of broader incidents being managed by the Sector, by inhibiting an effective response. Risk assessment SMEs identified various motivations criminals or others with malicious intent could have for impeding incident management capabilities, such as financial gain, intelligence gathering, or political projection. However, regardless of motivation, such actions are possible with operational-level skills, logical and/or physical access, and minimal resources. The types of actors can range from individuals internal or external to the Sector to more sophisticated organizations or—possibly—nation-states that are not bound by U.S. moral or legal code. Disgruntled employees could also interfere with the *Provide Incident Management Capabilities* function, highlighting the insider threat.

Unintentional threats to the function may come from employees or third party vendors, and may be a result of their lack of training. These actors' roles in this function would likely be in implementation, production, and manufacturing; requirements, design, R&D, and discovery; or delivery, deployment, and distribution. Common threat characteristics include significant physical and/or logical access to the function's assets, systems, and networks; and the likely use of a defective, misaligned, or an un-calibrated tool. Natural threats include those that could impact personnel and manufacturing such as epidemics or pandemics, droughts, and severe weather.

3 Provide Incident Management Capabilities Risk Management Strategy

This section describes the IT Sector SME-proposed risk management strategies for three of the function's risks. Those risks, as identified in the ITSRA, are:

- Impact to detection capabilities due to a lack or unavailability of risk-related data, which is caused by a natural hazard
- Impact to detection resulting from a manmade deliberate falsification of incident report data
- Impact to response capabilities due to a manmade deliberate exploitation of capabilities that prevent response or render the response ineffective

IT Sector partners resolved to pursue *Mitigate the risk by preventative action or the implementation of other risk reduction activities* as the selected response for all three of the identified risks.

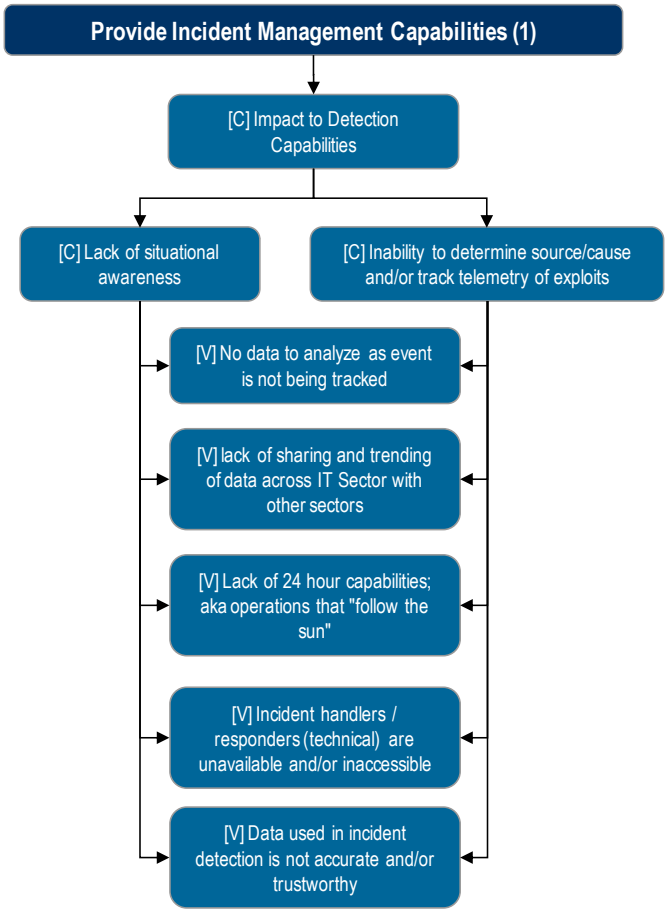
The following sections list and analyze activities that can reduce the specific risks identified in the ITSRA. In addition to these risk-specific mitigation activities, there are more general efforts underway that also reduce the risk profile of the *Provide incident management capabilities* function. Two of these main efforts include (1) the growth and maturity of national and sector level incident response capabilities and (2) the continued organization-level efforts to continuously evaluate and align incident management capabilities with the mission or business objectives of the organization they support.

3.1 Risk of Concern – Lack of Data: Impact to Detection (Natural)

3.1.1 Risk Overview

Figure 4 highlights vulnerabilities arising from a lack of data that, if exploited, would result in the consequence of an impact to the detection of an issue or degradation to the system. The attack tree provides the scope of the IT Sector's risk response strategy to this risk by illustrating how unavailability or lack of integrity of sensor data and information about incidents can result in a degradation of detection capabilities.

Figure 4: InM 1a: Impact to Detection – Lack of Data



3.1.2 Risk Strategy for Lack of Data: Impact to Detection (Natural)

The ITSRA established that the national-level risk of a natural occurrence to the detection capabilities of an issue is *medium likelihood* and *high consequence* (see Figure 3). IT Sector partners identified a combined mitigation strategy that includes:

- Redundancy and distribution of resources and data.
  - Disperse response capabilities
  - Distribute sources and content through the development of multiple databases in geographically disperse areas
  - Improve the access of data between databases and response personnel
- Move toward a federated model so that incident management capabilities are not completely centralized.
  - Explore the possibility of a distributed workforce
- Promote and support virtual work environments to ensure a remote workforce has access to data.
  - Businesses and organizations should promote and test work-from-home programs
  - Businesses and organizations should establish remote network access
- Clearly defining the roles of the Federal Government in responding to Significant Cyber Incidents.
  - Clearly define the role of Government in the National Cyber Incident Response Plan (NCIRP) and complementary cyber incident response documents to promote coordinated response efforts

- Further integrate the private sector into daily and incident-related NCCIC operations to increase the coordination between government and industry entities when detecting and responding to Significant Cyber Incidents

Incident response capabilities—both at the organization level as well as at sector or national coordination levels—have redundant and resilient infrastructures built into them already. As technology has evolved to address more sophisticated risks over the past several years, organizations have implemented approaches that reduce geographical and logical single points of failure. These entities regularly test and enhance these capabilities today, and they will continue to do so in the future to adapt to the risk environment of the future.

After formulating the combined risk mitigation strategy outline above, IT Sector partners noted that promoting these measures would have a positive impact across the broader IT Sector's critical functions. The enhanced redundancies would lead to an increase in the availability of products and services provided by each of the functions. Therefore, partners concluded that full nation-wide implementation of the proposed mitigation activities above would reduce the national-level risk beyond the improvements made directly in the *Provide Incident Management Capabilities* function.

Conversely, if these measures are not promoted or implemented, the likelihood of a threat exploiting incident management vulnerabilities will remain the same. The ITSRA, the source of the likelihood and concerns addressed in this report, was first drafted in 2009. Since a natural incident is the attribution of this risk, the likelihood of a threat successfully exploiting a vulnerability will not have significantly changed since 2009.

Table 2 shows the IT Sector partners' determinations of feasibility across several factors and the criteria by which those determinations were made.

Table 2: Feasibility of Proposed Mitigation Strategy to Lack of Data: Impact to Detection

Feasibility Factors	Feasibility	Description	Explanation
Legal	**High**	Statutes, regulation	The existing legal framework is extremely favorable for the implementation of the proposed risk response.
Organizational Compliance	**High**	Best practices, organizational charters, corporate values	In order to maintain and continue operations, almost all entities have developed best practices to protect against the exploitation of vulnerabilities. Therefore, the implementation of the proposed risk response aligns closely with the existing standards and best practices.
Political	**High**	Public confidence, privacy-related issues	There may be privacy concerns involved, however, changes will likely be deemed acceptable during an emergency incident.

Feasibility Factors	Feasibility	Description	Explanation
Financial	**Medium**	Cost, budget limitations	The cost of developing, implementing, and maintaining the proposed risk response could pose a strain on organizations already suffering from current market conditions. However, the cost of operational down time should prove as justification for the investment.
Time	**Medium**	Reasonable schedule expectations	The implementation of the proposed risk response can be completed in a reasonable time frame (i.e., 13-24 months to full implementation).
Technology	**High**	Ease of implementing existing technology or developing new technology	The technology is readily available for implementation with no need for extensive R&D prior to execution.
Market	**High**	Market conditions, competition	Organizations are already implementing strategies that include these mitigation activities, and for those who have already done so, they continue to find ways to make their detection capabilities more resilient.
Compatibility	**Medium**	Confidentiality, Integrity, and Availability after implementation	Compatibility issues associated with this risk response would include VPN services, additional data routing, and server capacity. These and other factors would need to be addressed during plan development.
Cultural	**High**	The alignment of IT Sector culture and the risk response	As discussed above, organizations are already implementing a portion of the proposed risk response so the current environment is favorable.

3.2 Risk of Concern – Falsified Reports: Impact to Detection (Manmade Deliberate)

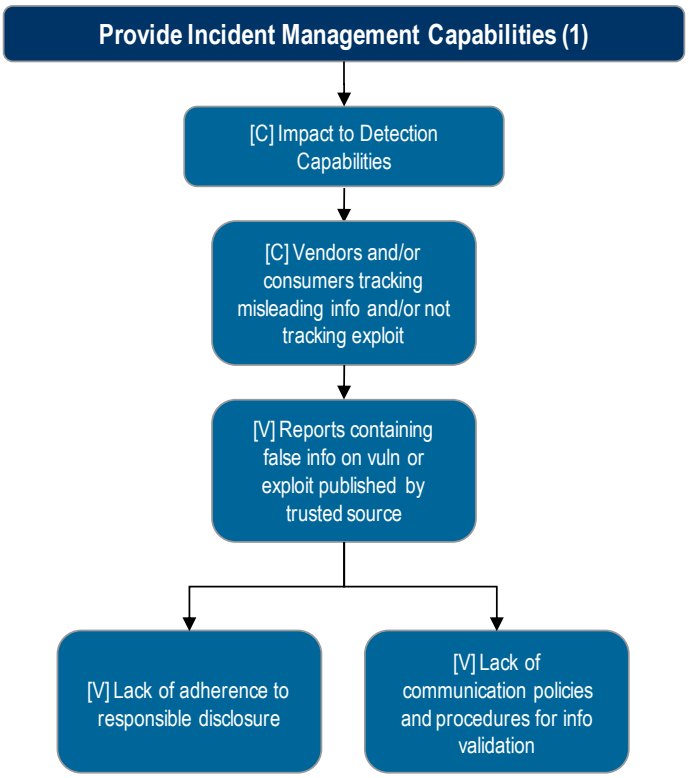
3.2.1 Risk Overview

A failure to recognize falsified reports is a serious risk to the IT Sector incident management function and could significantly hinder the detection of incidents that cause major economic and national security consequences. As noted in the ITSRA, incident responders mistakenly using misinformed or inaccurate data to track and trend an event could have a significant impact on identifying and (as a result) managing

an incident. The successful distribution of falsified information is likely to occur covertly and likely to be conducted by actors who are sophisticated, well-organized, and probably associated with larger entities such as nation-states or crime syndicates.[3] Threat actors could include corporate spies, corrupt government officials, cyber vandals, disgruntled employees, foreign government agents or spies, nation-states, radical activists, and criminals. These threat actors can be motivated by a variety of concerns, such as financial gain, state-sponsored or corporate-sponsored disruption, or the desire to project power. Severe risks could be caused by trusting falsified reports as well as a lack of adherence to established data collection and analysis processes.

Risk assessment SMEs created the attack tree shown below in Figure 5 to scope the IT Sector's risk response strategy to this risk.

Figure 5: InM 1b: Impact to Detection – Falsified Reports



3.2.2 Risk Strategy for Falsified Reports: Impact to Detection (Manmade)

The ITSRA established that the national-level risk of a manmade, deliberate falsified report to the detection capabilities of an issue is *low likelihood* and *low consequence* (see Figure 3). IT Sector partners reached a consensus viewpoint that IT Sector organizations should address this risk through implementing a combined mitigation strategy, including:

[3] For the purposes of this analysis, the report focuses on deliberate falsification of information. There are also risks associated with accidently creating false reports, but the strategy for addressing such a risk varies enough that those activities are not the focus of this section.

- Distribution/integrity check on data; Multiple primary sources.
- Education of the workforce to recognize falsified information and validate sources: Training and awareness.
- Vet existing reports to screen out false reports.

These activities can be accomplished with the resources available to the IT Sector today and would not likely require research and development.

After formulating the combined risk mitigation strategy, IT Sector partners noted that the proposed strategy outlined above would have an overall positive impact to the critical function and decrease the likelihood of a false report being disseminated to incident management stakeholders. After reviewing the other IT Sector functions, it was found that their own incident management capabilities could be positively impacted by the identified risk strategy. On an organizational level, these measures could provide a positive impact to internal incident management practices as well. Therefore, partners concluded that full nation-wide implementation of the proposed mitigation activities above would reduce the national-level risk beyond the improvements made directly in the *Provide Incident Management Capabilities* function.

Conversely, if these measures are not implemented, the likelihood of a threat exploiting incident management vulnerabilities will increase or remain the same. The ITSRA, the source of the likelihood and concerns addressed in this report, was first drafted in 2009. Since that time, threats have grown more sophisticated as adversaries improve their capabilities. Even though the sector continues to mitigate this risk, the consequences have not changed, and incident management remains a target for malicious action.

Table 3 shows the IT Sector partners' determinations of feasibility across several factors and the criteria by which those determinations were made.

Table 3: Feasibility of Proposed Mitigation Strategy to Lack of Data: Impact to Detection

Feasibility Factors	Feasibility	Description	Explanation
Legal	**High**	Statutes, regulation	The existing legal framework is extremely favorable for the implementation of the proposed risk response.
Organizational Compliance	**High**	Best practices, organizational charters, corporate values	In order to maintain and continue operations, almost all entities have developed best practices to protect against the exploitation of vulnerabilities. Therefore, the implementation of the proposed risk response will likely align closely with existing standards and best practices.
Political	**High**	Public confidence, privacy-related issues	There may be privacy concerns involved, however, changes will likely be deemed acceptable during an emergency incident.

Feasibility Factors	Feasibility	Description	Explanation
Financial	**Medium**	Cost, budget limitations	The cost of developing, implementing, and maintaining the proposed risk response could pose a strain on organizations already suffering from current market conditions. However, the loss of public confidence due to a falsified report should prove as an incentive for the investment.
Time	**Medium**	Reasonable schedule expectations	The implementation of the proposed risk response can be completed in a reasonable time frame (i.e., 13-24 months to full implementation).
Technology	**High**	Ease of implement existing technology or developing new technology	The technology is available for immediate implementation.
Market	**High**	Market conditions, competition	Organizations are already implementing strategies that include these mitigation activities, and for those who have already done so, they continue to find ways to make their detection capabilities more resilient.
Compatibility	**Medium**	Confidentiality, Integrity, and Availability after implementation	Compatibility issues associated with this risk response would include VPN services, additional data routing, and server capacity. These and other factors would need to be addressed during plan development.
Cultural	**High**	The alignment of IT Sector culture and the risk response	As discussed above, organizations are already implementing a portion of the proposed risk response so the current environment is favorable.

3.3 Risk of Concern – Incident Response Prevented or Rendered Ineffective: Impact to Response (Manmade Deliberate)

3.3.1 Risk Overview

The inability to prevent incident management or render it ineffective is a serious threat to the IT Sector incident management function. A lack of common situational awareness among incident responders could leave critical assets, systems, networks, and functions vulnerable. This lack of situational awareness could be due to manmade threats that prohibit key response personnel from accessing key incident data.

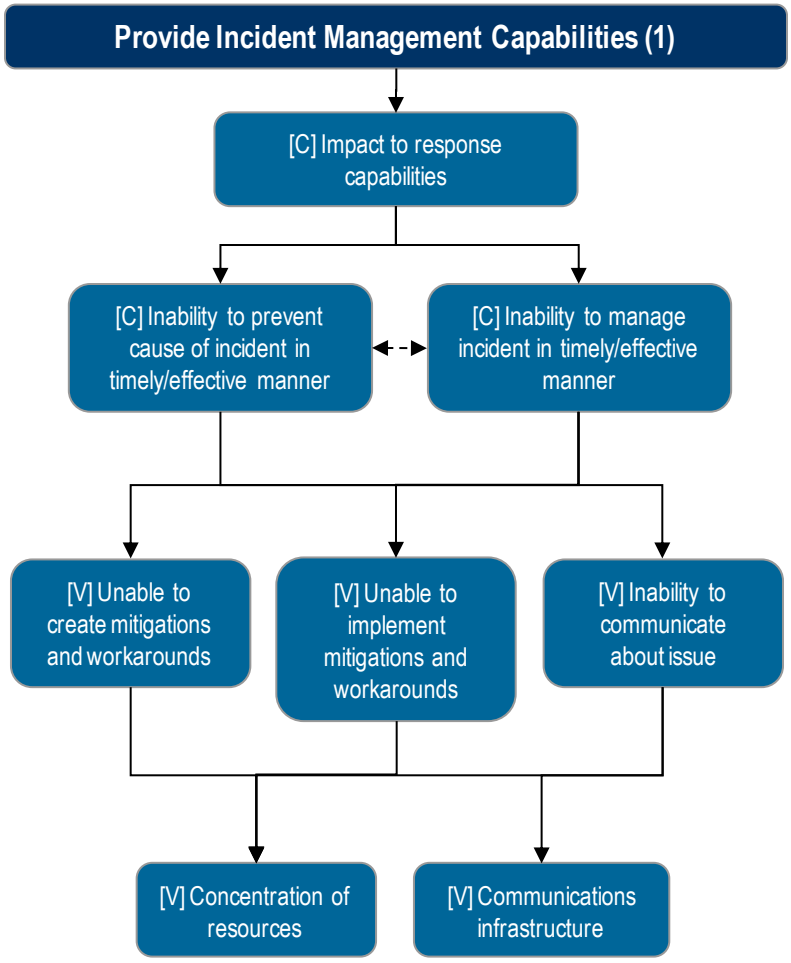
Additionally, the inability to determine the source or the cause of an incident could prevent an effective response. Several vulnerabilities could exacerbate these concerns, including a lack of data to analyze if the incident is not being tracked; a lack of sharing and trending of data across the Sector and with other sectors; a possible gap in 24-hour incident management capability; a lack of availability of incident handlers and technical responders caused by manmade or natural events; and inaccurate or untrustworthy data used in incident detection.

In recent years there have been several high-profile examples of this risk. For example, on January 25, 2003 the SQL Slammer Worm caused a denial of service to over 75,000 Internet hosts in less than 10 minutes.[4] The Slammer Worm spread considerably faster than other similar worms, such as the Code Red worm from 2001.[5] On July 4, 2009, a widespread denial of service attack inundated U.S. government and South Korean websites.[6] The incident temporarily paralyzed several U.S. government networks. Similar incidents occurred in Estonia in 2007[7] and in Georgia in 2008.[8]

Risk assessment SMEs created the attack tree shown below in Figure 6 to identify vulnerabilities arising from the inability to respond to an incident, or only to mount an ineffective response. The attack tree provides the scope of the IT Sector's risk response strategy to this risk.

[4] For more information, please see http://www.cert.org/advisories/CA-2003-04.html
[5] For more information, please see http://www.cert.org/advisories/CA-2001-19.html
[6] For more information, please see http://www.networkworld.com/news/2009/071009-korea-ddos-virus-mission-shifts.html
[7] For more information, please see http://www.msnbc.msn.com/id/31801246/ns/technology_and_science-security
[8] For more information, please see http://www.nytimes.com/2008/08/13/technology/13cyber.html

Figure 6: InM 2: Impact to Response – Response Prevented or Rendered Ineffective



3.3.2 Risk Strategy for Incident Response Prevented: Impact to Response

The ITSRA established that the national-level risk of a manmade, deliberate interference that prevents incident response in a timely manner is *negligible likelihood* and *medium consequence* (see Figure 3). IT Sector partners reached a consensus viewpoint that a combined mitigation strategy should be chosen as the appropriate risk response to this particular risk of concern, including:

- Enhance training and awareness surrounding the capture of information to develop lessons learned for producers and providers of hardware and software services.
- Invest in or develop alternative data delivery capabilities in case primaries are unavailable.
- Distribute response resources so they are not all negatively impacted by the same incident.
- Build additional redundancies into current incident management infrastructure and resources.

After formulating the combined risk mitigation strategy, IT Sector partners noted that the proposed measures would have an overall positive impact to the critical function and its sub-functions. The development of redundancies could potentially impact the other functions negatively due to the additional flow of data; however, this development could also lend itself to a quicker recovery across the broader IT Sector. The implementation of lessons learned will result in a positive impact on the Provide Incident

Management Capabilities critical function. Therefore, partners concluded that full nation-wide implementation of the proposed mitigation activities above would reduce the national-level risk beyond the improvements made directly in the *Provide Incident Management Capabilities* function.

Table 4 shows the IT Sector partners' determinations of feasibility across several factors and the criteria by which those determinations were made.

Table 4: Feasibility of Proposed Mitigation Strategy to Impact to Response – Response Ineffective or Prevented

Feasibility Factors	Feasibility	Description	Explanation
Legal	**High**	Statutes, regulation	The existing legal framework is extremely favorable for the implementation of the proposed risk response.
Organizational Compliance	**High**	Best practices, organizational charters, corporate values	In order to maintain and continue operations, almost all entities have developed best practices to protect against the exploitation of vulnerabilities. Therefore, the implementation of the proposed risk response will likely align closely with existing standards and best practices.
Political	**High**	Public confidence, privacy-related issues	The proposed risk response would pose no threat to public confidence or provide privacy issues.
Financial	**Low**	Cost, budget limitations	The proposed risk response would not be covered via market forces or existing business models and may prove too costly for most organizations at this time.
Time	**Low**	Reasonable schedule expectations	The implementation of the proposed risk response will take a relatively longer time frame (i.e., 24 months or longer for full implementation).
Technology	**High**	Ease of implementing existing technology or developing new technology	The technology is available for immediate implementation.

Feasibility Factors	Feasibility	Description	Explanation
Market	**Medium**	Market conditions, competition	Organizations already implementing strategies that include these mitigation activities, and for those who have already done so, will continue to find ways to make their detection capabilities more resilient. Their successes will create more favorable conditions for more wide-spread implementation.
Compatibility	**Medium**	Confidentiality, Integrity, and Availability after implementation	Compatibility issues associated with this risk response would include VPN services, additional data routing, and server capacity. These and other factors would need to be addressed during plan development.
Cultural	**Medium**	The alignment of IT Sector culture and the risk response	The current cultural environment has the potential for facilitating the proposed risk response. As discussed above, successes within organizations already implementing a portion of the proposed risk response will produce a more favorable climate for wide spread implementation.

4 Results: Risk and Mitigation Overview

IT Sector partners analyzed the ITSRA risks of concern to the *Provide Incident Management Capabilities* critical function and developed mitigation responses to three risks of concern. The risks, associated RMAs, and resulting likelihood and consequence ratings appear in the table below.

Table 5: Risk and Mitigation Overview

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings[9]
Lack of Data: Impact to Detection	Medium likelihood; Medium consequence	• Duplicate geographically distinct storage areas • Move toward federated model so that incident management is executed by multiple entities and not only by the same entity impacted • Work virtually and promote remote work environments • Disperse response capabilities • Distribute sources and content (develop multiple databases in geographically disperse areas) • Improve the way to move data (how to move data between dispersed databases and response personnel) • Clearly define the role of the U.S. Government in responding to significant cyber incidents	Low likelihood; Medium consequence
Reports Containing False Information on a Vulnerability or Export: Impact to Detection	Medium likelihood; Medium consequence	• Conduct distribution/integrity check on data (finding multiple primary sources) • Educate workforce to recognize falsified information and validate sources (training and awareness) • Vet existing reports to screen out false reports	Low likelihood; Medium consequence
Incident Response Prevented or Rendered Ineffective in a Timely Manner: Impact to Response	Low likelihood; Medium consequence	• Enhance training and awareness surrounding the capture of information to develop lessons learned for producers and providers of hardware and software services • Invest in or develop alternative incident management infrastructure and resources in case primaries are unavailable • Distribute response resources so they are not all negatively impacted by the same incident • Build additional redundancies into current incident management infrastructure and resources	Low likelihood; Low consequence

9 Assumes complete implementation of the items noted in the Risk Mitigation Activities column.