Cyber Event affecting Data (Data as Target)

A cyber event[1] occurs which seriously compromises the integrity or availability of data (the information contained in a computer system) or data processes, resulting in economic losses of $1 billion or greater.

Data Summary

Category	Description	Metric	Low	Best	High
Health and Safety	Fatalities	Number of Fatalities	Not determined		
	Injuries and Illnesses	Number of Injuries or Illnesses	Not determined		
Economic	Direct Economic Loss	U.S. Dollars (2011)	Not determined		
Social	Social Displacement	People Displaced from Home ≥ 2 Days	0		
Psychological	Psychological Distress	Qualitative Bins	See text		
Environmental	Environmental Impact	Qualitative Bins[2]	None[3]		
LIKELIHOOD	Frequency of Events	Number of Events per Year	See classified data table		

Event Background

This category includes cyber attacks that focus on compromising data or data processes as the primary result. Such attacks could take many forms and be perpetrated in order to achieve many goals. Some examples might include the altering of records in a healthcare or financial system or an attack which causes the internet, communications networks, or data processes to cease.

While frequency information about the type of data/data processes attacks included in this category is difficult to locate in open source material, there are several observations that can assist in setting the context.

A 2010 Verizon report analyzing 141 data breach cases from 2009 (worked by either the Verizon Investigative Response Team or the U.S. Secret Service) estimated the total number of data records compromised across these cases to exceed 143 million.[4] Consistent with previous years, most of the losses in 2009 came from only a few of the 141 breaches. The average number of records lost per breach was 1,381,183, the median only 1,082, and the standard deviation 11,283,151.[5]

[1] The Cyber Attack against Data national-level event was renamed Cyber Event affecting Data in 2013 to address stakeholder concerns.
[2] The United States Environmental Protection Agency (EPA) convened an ad hoc group of environmental experts representing the fields of environmental science, ecological risk, toxicology, and disaster field operations management to estimate environmental impacts for this event. The comments and rankings presented in this Risk Summary Sheet have not undergone review by the EPA and only represent the opinions of the group. Estimates pertain to the potential for adverse effects on living organisms associated with pollution of the environment; they are grouped into high, moderate, low, and *de minimus* (none) categories.
[3] Experts provided both first and second choice categories, allowing the experts to express uncertainty in their judgments as well as reflect the range of potential effects that might result depending on the specifics of the event. The first choice represents the 'Best' estimate.
[4] Verizon RISK Team, 2010 Data Breach Investigations Report (2010): 7.
[5] Ibid.: 40.

In the case of denial-of-service events, according to a 2010 CSIS-McAfee survey of 200 critical infrastructure executives from the energy, oil/gas, and water sectors in 14 countries, nearly 80 percent of the respondents reported facing a large-scale denial-of-service attack in 2010 (up from just over half in 2009), with a quarter reporting daily or weekly denial-of-service attacks on a large scale.[6]

Additionally, one in four of the CSIS-McAfee respondents said they had been the victim of extortion through attack or threat of attack to IT networks in the past two years—an increase from one in five respondents from the previous year.[7]

Impacts for the types of attacks in this event category are difficult to quantify, as they depend on the particular system attacked, the vulnerability and resilience of the network, specific data backup provisions, and other factors. A sample of several historical data/data processes-related cyber attacks is presented in the "Additional Relevant Information" section below. In addition, details on the Wall Street "Flash Crash" are included in the list, in order to provide context on the potential magnitude of impacts produced by events in this category.

Assumptions

Likelihood

Frequency estimates were elicited from the Intelligence Community (IC) by the SNRA project team in July-August 2011.[8] Only attacks resulting in $1 billion in losses or greater were considered. The frequency estimates for this event are classified, but are provided in the data tables of the classified SNRA Technical Report.

Frequency estimates were based on the following assumptions regarding the scope of events in this category.

- General Scope: This category includes cyber attacks that focus on compromising data or data processes as the primary result. Although events in this category almost always have indirect effects that "go beyond the computer," only events in which these types of effects are a function of modern reliance on computer systems—rather than the primary objective of the attack—were considered.
- Actor Types: Given the goal of capturing the full range of national-level possibilities within each type of incident, events in which cyber attacks are intentionally caused by any type of human actor, including, e.g., hackers, activists, states, terrorists, malicious insiders, or criminals, were considered. Unintentional human-caused events (such as unintentional breaches or accidents) or non-human-caused events (such as those caused by natural disasters or equipment malfunctions) were not considered.
- Weapon Types: All types of cyber weapons, including but not limited to malicious software, botnets, distributed denial-of-service attacks, etc., were considered.
- Target Types: Any type of civilian target was considered. Note that for the purposes of the SNRA—which is intended to inform civilian capability development—direct attacks on

[6] McAfee and the Center for Strategic and International Studies, *In the Dark: Crucial Industries Confront Cyberattacks* (April 2011): 6.
[7] Ibid.
[8] IC participants in the Cyber Event affecting Data frequency elicitation included subject matter experts from multiple agencies. The frequency estimates (see classified SNRA Technical Report) reflect the opinion of the group and have not been formally vetted by any of the agencies which participated.

defense systems were not considered. Additionally, state- and non-state- sponsored espionage was not considered.

- Time Period: The SNRA focuses on estimating risk within the next five years, in support of the overall need to focus on future-oriented core capability development.
- National-level Threshold: As stated above, the SNRA is designed to assess the risks of those events and incidents which create impacts that rise to a strategic, national-level of impact. Thus, small-scale attacks, which occur on a daily basis, were not considered. Instead, only high-impact events, which could produce a national level of awareness due to major impacts related to life safety, economic damage, psychological damage, social displacement, or environmental damage were considered.

Fatalities, Injuries and Illnesses, Economic Damage

Defensible estimates could not be obtained on these impact measures. Additional analysis will be needed to quantify the human health and economic impacts of the Cyber Event affecting Data event.

Psychological Distress

Since the SNRA measure of psychological distress is tied to fatality and illness/injury estimates, psychological distress estimates were not reported in the SNRA for the Cyber Event affecting Data national-level event.[9]

Social Displacement

For the purposes of the SNRA, social displacement was defined as the number of people forced to leave home for a period of two days or longer. Note that there are limitations to this measure of social displacement, as the significant differences between temporary evacuations and permanent displacement due to property destruction are not captured.

- As the Cyber Event affecting Data national-level event is restricted to cyber events not directly causing impacts on the physical world, the SNRA project team assessed the low, best, and high estimates for social displacement to be zero.

Environmental Impact

The United States Environmental Protection Agency (EPA) convened an ad hoc group of environmental experts representing the fields of environmental science, ecological risk, toxicology, and disaster field operations management to estimate environmental impacts for this event. Estimates are based on the following assumptions:

[9] The SNRA measures psychological distress by a Significant Distress Index calculated from fatality, illness/injury, and social displacement estimates using a formula proposed by subject matter experts consulted for the SNRA project: $N_{SD} = C_{EF} \times (5\ Fat + Inj + \frac{1}{2}\ D)$, where N_{SD} represents the number of persons significantly distressed, C_{EF} is an expert assessed Event Familiarity Factor, *Fat* is the number of fatalities, *Inj* is the number of injuries and/or illnesses, and *D* is the number of persons displaced (Social Displacement). In words, this formula suggests that there are 5 significantly distressed persons for each life lost; 1 for each person injured; and 1 for each 2 people displaced. This formula was constructed to reflect the empirical finding that the most severe stressor of a disaster is losing a loved one, followed by injury, followed by displacement. Uncertainty was captured by applying the index formula to the low, best, and high estimates of these three human impact metrics.

The Event Familiarity Factor is intended to capture the extent to which the event entails an ongoing threat with uncertainty regarding long term effects, is unfamiliar, or that people dread, exacerbating psychological impacts. This factor, ranging from 1.0 for familiar events to 1.3 for unfamiliar events, was provided by subject matter experts for each national-level event included in the SNRA: experts assessed a C_{EF} of 1.0 for the Cyber Event affecting Data national-level event.

Although the SNRA determined null social displacement estimates for the Cyber Event affecting Data, scenarios which could credibly threaten human health and safety without forcing people to flee their homes remained part of the event scope and so the SNRA project team could not assume zero estimates for fatalities and illnesses/injuries as well.

- Experts were elicited to provide estimates in the environmental impact category based on assumptions. Actual environmental/ecological harm that occurs as a result of the events described in a given scenario may vary considerably, and will depend on numerous variables (e.g., chemical or biological agent, contamination extent, persistence, toxicity—both chronic and acute toxicity—and infectivity).
- EPA defined environmental consequence (impact)[10] as the potential for adverse effects on living organisms associated with pollution of the environment by effluents, emissions, wastes, or accidental chemical releases; energy use; or the depletion of natural resources.
- Experts identified the best estimate for environmental impacts as "de minimus" or none.

Potential Mitigating Factors

The risk of this type of cyber attack can be mitigated through several preparedness strategies. Practices such as employing advanced authentication measures, the use of encryption technologies, and the monitoring of network use for anomaly detection would help to prevent, more quickly identify, and facilitate a timely response to cyber attacks.[11] In addition, organizations can employ tailored strategies that increase resilience to cyber attacks on data. These could include strategies such as employing back-up systems and developing plans for maintaining operations without the use of computer systems.

Additional Relevant Information

A sample list of several historical data/data processes related to cyber attacks is presented below. Details on the Wall Street "Flash Crash" are included in the list, in order to provide context on the potential magnitude of impacts produced by events in this category.

Attacks on Data and the Potential Magnitude of Compromised Data Integrity or Accessibility[12]
Seattle Hospital Denial of Access. Cyber criminals in 2007 compromised the networks of a Seattle hospital, causing system malfunctions including the crash of the Intensive Care Unit Network.
Wall Street "Flash Crash." In Wall Street's May 2010 "flash crash," complex automated trades created enough market volatility to hemorrhage approximately 1 trillion dollars in only minutes, with some stocks dropping more than 90 percent in value. While the volatility was unintentional and the stocks recovered, the crash illustrates the potential impacts of sophisticated cyber attacks against a financial system that relies increasingly on automated high-frequency trading.[13]

[10] The 2011 SNRA referred to impacts as 'consequences' because of prior usage in quantitative risk assessment (Kaplan and Garrick [1981, March], On the quantitative definition of risk: *Risk Analysis* 1(1) 11-32). Except where it will cause confusion, 'impact' is used synonymously in this document because of pre-existing connotations of the word 'consequence' within FEMA.
[11] See McAfee and the Center for Strategic and International Studies: 24.
[12] This list was provided to the participants in the frequency elicitation, to encourage consideration of potential impacts of a cyber attack against data.
[13] Quoted in full from David Pett, "High-Frequency Swaps, Dark Pools Under Scrutiny," *National Post's Financial Post & FP Investing* (8 May 2010) and Kara Scannell and Tom Lauricella, "Flash Crash Is Pinned On One Trade," *The Wall Street Journal* (2 October 2010) as cited in Lord and Sharp: 1:25.

Additional References

Clem et al (2003). Health implications of cyber-terrorism. *Prehospital and Disaster Medicine* 18(3) 272-275.

Congressional Research Service (2007, January 22). Terrorist capabilities for cyberattack: overview and policy issues. CRS Report to Congress RL33123, Congressional Research Service, Library of Congress; at http://www.fas.org/sgp/crs/terror/RL33123.pdf (checked April 2013).

Lewis, James A. (2002, December). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Center for Strategic and International Studies; at http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (checked April 2013).

Lewis, James A (2011). Cybersecurity: assessing the immediate threat to the United States. Statement before the House Oversight and Government Reform Committee, Subcommittee on National Security, Homeland Defense, and Foreign Operations, May 25, 2011. Center for Strategic & International Studies (CSIS); at http://csis.org/testimony/cybersecurity-assessing-immediate-threat-united-states (checked April 2013).

Lewis, James A (2011). Examining the Cyber Threat to Critical Infrastructure and the American Economy. Statement before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, March 16, 2011. Center for Strategic & International Studies (CSIS); at http://csis.org/testimony/examining-cyber-threat-critical-infrastructure-and-american-economy (checked April 2013).

McAfee and the Center for Strategic and International Studies (April 2011). In the Dark: Critical Industries Confront Cyberattacks [McAfee second annual critical infrastructure protection report]; at http://www.mcafee.com/cip_report (checked April 2013).

McConnell, Mike (2011). Cyber insecurities: the 21st century threatscape. In Kahn et al, America's Cyber Future: Security and Prosperity in the Information Age (Chapter II). Center for a New American Security, May 31, 2011.

McGraw, Gary, Nathaniel Fick (2011). Separating threat from the hype: what Washington needs to know about cyber security. In Kahn et al, America's Cyber Future: Security and Prosperity in the Information Age (Chapter III). Center for a New American Security, May 31, 2011.

Nye, Joseph S, Jr. (2011). Power and national security in cyberspace. In Kahn et al, America's Cyber Future: Security and Prosperity in the Information Age (Chapter I). Center for a New American Security, May 31, 2011.

Organization for Economic Co-operation and Development (OECD) (2011, January 14). Reducing systemic cybersecurity risk. Report IFP/WKP/FGS(2011)2, OECD/International Futures Programme (IFP) Project on "Future Global Shocks"; at http://www.oecd.org/dataoecd/57/44/46889922.pdf (checked April 2013).

Schroeder, Christopher M. (2011). The unprecedented economic risks of network insecurity. In Kahn et al, America's Cyber Future: Security and Prosperity in the Information Age (Chapter X). Center for a New American Security, May 31, 2011.

Sumner, Mary (2009, January). Information security threats: a comparative analysis of impact, probability, and preparedness. *Information Systems Management* 26(1) 2-12.

U.S. Department of Homeland Security (2011, August). Information Technology Sector Baseline Risk Assessment; at http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf (checked April 2013).

Cyber Event affecting Physical Infrastructure

A cyber event in which cyber means are used as a vector to achieve effects which are "beyond the computer" (i.e., kinetic or other effects), resulting in one or more fatalities or economic losses of $100 million or more.

Data Summary

Category	Description	Metric	Low	Best	High
Health and Safety	Fatalities	Number of Fatalities	Not determined		
	Injuries and Illnesses	Number of Injuries or Illnesses	Not determined		
Economic	Direct Economic Loss	U.S. Dollars (2011)	Not determined		
Social	Social Displacement	People Displaced from Home ≥ 2 Days	0	400	Not determined
Psychological	Psychological Distress	Qualitative Bins	See text		
Environmental	Environmental Impact	Qualitative Bins[1]	None[2]		
LIKELIHOOD	Frequency of Events	Number of Events per Year	See classified data table		

Event Background

This category encompasses cyber attacks that directly produce national-level effects outside the virtual world. These types of events could involve a variety of targets, such as large-scale assets in a variety of critical infrastructure sectors. Examples might include the electric grid, a dam, or the water system.

The threat of this type of event has seen increased prominence recently, as the extent of the Stuxnet infections have come to light. According to a 2010 CSIS-McAfee survey of 200 critical infrastructure executives from the energy, oil/gas, and water sectors in 14 countries, around 40 percent of respondents found Stuxnet on their computers.[3] While three-quarters of respondents who found Stuxnet were confident it has been removed from their systems, the potential for widespread sabotage through the introduction of malware into SCADA systems was clearly demonstrated.[4] The 2007 "Aurora" tests conducted at Idaho National Labs further confirmed the proposition that hackers could gain remote access to a control system and, in that case, remotely change the operating cycle of a generator, sending it out of control.[5]

[1] The United States Environmental Protection Agency (EPA) convened an ad hoc group of environmental experts representing the fields of environmental science, ecological risk, toxicology, and disaster field operations management to estimate environmental impacts for this event. The comments and rankings presented in this Risk Summary Sheet have not undergone review by the EPA and only represent the opinions of the group. Estimates pertain to the potential for adverse effects on living organisms associated with pollution of the environment; they are grouped into high, moderate, low, and de minimus (none) categories.
[2] Experts provided both first and second choice categories, allowing the experts to express uncertainty in their judgments as well as reflect the range of potential effects that might result depending on the specifics of the event. The first choice represents the 'Best' estimate.
[3] McAfee and the Center for Strategic and International Studies, *In the Dark: Crucial Industries Confront Cyberattacks* (April 2011): 8.
[4] Ibid.
[5] James A. Lewis, "The Electrical Grid as a Target for Cyber Attack," Center for Strategic and International Studies (March 2010).

More than 40 percent of the executives interviewed in the CSIS-McAfee survey reported they expected a major cyber attack within 12 months—i.e., an attack that would cause severe loss of services for at least 24 hours, a loss of life or personal injury, or the failure of a company.[6] It should be noted, however, that the types of attacks cited in the study—though important for individual companies—would not necessarily produce impacts that would rise to the threshold for a national-level event.

Impacts for the types of attacks in this event category are sector dependent and difficult to quantify. Approximately 85% of critical infrastructure is believed to be owned and operated by the private sector, and system vulnerability and resilience is highly sector-dependent and localized.[7] A sample of historical attacks on the SCADA systems of critical infrastructure assets, along with a list of unintentional or non-cyber related failures within critical infrastructure sectors is included in the "Additional Relevant Information" section below.

Assumptions

Likelihood

Frequency estimates were elicited from the Intelligence Community (IC) by the SNRA project team in July-August 2011.[8] Only attacks resulting in one or more fatalities, or $100 million in losses or greater were considered. The frequency estimates for this event are classified, but are provided in the data tables of the classified SNRA Technical Report.

Frequency estimates were based on the following assumptions regarding the scope of events in this category:

- **General Scope:** This event encompasses cyber attacks that directly produce national-level effects outside the virtual world. While the attacks in this category may involve the manipulation of data as a means to an end, an event whose direct result is only compromised data (such as intellectual property theft or altered healthcare records) was not considered.
- **Actor Types:** Given the goal of capturing the full range of national-level possibilities within each type of incident, events in which cyber attacks are intentionally caused by any type of human actor, including, e.g., hackers, activists, states, terrorists, malicious insiders, or criminals, were considered. Unintentional human-caused events (such as unintentional breaches or accidents) or non-human-caused events (such as those caused by natural disasters or equipment malfunctions) were not considered.
- **Weapon Types:** All types of cyber weapons, including but not limited to malicious software, botnets, distributed denial-of-service attacks, etc., were considered.
- **Target Types:** Any type of civilian target was considered. Note that for the purposes of the SNRA—which is intended to inform civilian capability development—direct attacks on defense systems were not considered. Additionally, state- and non-state- sponsored espionage was not considered.

[6] McAfee and the Center for Strategic and International Studies: 10.
[7] According to the Office of Infrastructure Protection, Department of Homeland Security. http://www.dhs.gov/files/partnerships/editorial_0206.shtm.
[8] IC participants in the Cyber Event affecting Physical Infrastructure frequency elicitation included subject matter experts from multiple agencies. The frequency estimates (see classified SNRA Technical Report) reflect the opinion of the group and have not been formally vetted by any of the agencies which participated.

- **Time Period:** The SNRA focuses on estimating risk within the next five years, in support of the overall need to focus on future-oriented core capability development.
- **National-level Threshold:** As stated above, the SNRA is designed to assess the risks of those events and incidents which create impacts that rise to a strategic, national-level of impact. Thus, small-scale attacks, which occur on a daily basis, were not considered. Instead, only high-impact events, which could produce a national level of awareness due to major impacts related to life safety, economic damage, psychological damage, social displacement, or environmental damage were considered.

Fatalities, Injuries and Illnesses, Economic Damage

Defensible estimates could not be obtained on these impact measures. Additional analysis will be needed to quantify the human health and economic impacts of the Cyber Event affecting Physical Infrastructure event.

Social Displacement

For the purposes of the SNRA, social displacement was defined as the number of people forced to leave home for a period of two days or longer. Note that there are limitations to this measure of social displacement, as the significant differences between temporary evacuations and permanent displacement due to property destruction are not captured.

- Low and best estimates of social displacement estimates for the Cyber Event affecting Physical Infrastructure national-level event were provided by the National Consortium for the Study of Terrorism and Responses to Terrorism (START).[9] The low estimate of 0 reflects assessed judgment of START subject matter experts. The best estimate of 400 comes from a case study of an evacuation of an U.S. Army base due to a large but accidental power outage: this historical event was considered a reasonable proxy for displacement due to an intentional power outage following a cyber attack on the electrical grid.[10]
- No high estimate was determined. However, START subject matter experts noted that a cyber event causing a prolonged power outage over a large area could result in several thousand people evacuating, regardless of the outage cause.

Psychological Distress

Psychological impacts for the SNRA focus on *significant distress* and *prolonged distress*, which can encompass a variety of outcomes serious enough to impair daily role functioning and quality of life. An index for significant distress was created that reflected empirical findings that the scope and severity of an event is more important than the type of event. The equation for this index uses the fatalities, injuries, and displacement associated with an event as primary inputs; a factor elicited from subject matter experts weights the index for differing psychological impact based on the type of event, but as a secondary input.[11] The numerical outputs of this index

[9] START is a Department of Homeland Security University Center of Excellence that focuses on social and behavioral aspects of terrorism, natural disasters, and technological accidents, and the social, behavioral, cultural and economic factors influencing responses to and recovery from catastrophes.

[10] Reed, Charlie and Grant Okubo. "Flooding, power outages force evacuations at Yokota." *Stars and Stripes* (July 6, 2010). http://www.stripes.com/news/pacific/japan/flooding-power-outages-force-evacuations-at-yokota-1.110071.

[11] The Significant Distress Index is calculated from these inputs using a formula proposed by subject matter experts consulted for the SNRA project: $N_{SD} = C_{EF} \times (5\ Fat + Inj + \frac{1}{2}\ D)$, where N_{SD} represents the number of persons significantly distressed, C_{EF} is an expert assessed Event Familiarity Factor, *Fat* is the number of fatalities, *Inj* is the number of injuries and/or illnesses, and *D* is the number of persons displaced (Social Displacement). In words, this formula suggests that there are 5 significantly distressed persons for each life lost; 1 for each person injured; and 1 for each 2 people displaced. This formula was constructed to reflect the empirical finding that the most severe stressor of a disaster is losing a loved one, followed by

formula were used to assign events to bins of a risk matrix for a semi-quantitative analysis of psychological risk in the SNRA.

Environmental Impacts

The United States Environmental Protection Agency (EPA) convened an ad hoc group of environmental experts representing the fields of environmental science, ecological risk, toxicology, and disaster field operations management to estimate environmental impacts for this event. Estimates are based on the following assumptions:

- Experts were elicited to provide estimates in the environmental impact category based on assumptions. Actual environmental/ecological harm that occurs as a result of the events described in a given scenario may vary considerably, and will depend on numerous variables (e.g. chemical or biological agent, contamination extent, persistence, toxicity—both chronic and acute toxicity—and infectivity).
- EPA defined environmental consequence (impact)[12] as the potential for adverse effects on living organisms associated with pollution of the environment by effluents, emissions, wastes, or accidental chemical releases; energy use; or the depletion of natural resources.
- Experts identified the best estimate for environmental impacts as "de minimus" or none. Experts indicated, however, that this depends on the duration of the event. If the impacts of the event (e.g., power outages) occur for longer than a few days, then backup systems for sewage plants, chemical facilities, etc. could fail and result in more severe environmental impacts.

Potential Mitigating Factors

The risk of this type of cyber attack can be mitigated through preparedness strategies that act on both cyber systems and the actual target itself. Cyber strategies include practices such as the use of encryption technologies and the monitoring of network use for anomaly detection.[13] Target specific strategies include the range of measures that are typically employed to manage the risk to critical infrastructure systems. These will vary from sector to sector, but, in general, strategies to increase resilience will likely assist in mitigating the impacts from this type of cyber attack, as well as other threats and hazards.

Additional Relevant Information

A sample of historical attacks on the SCADA systems of critical infrastructure assets is presented below, in order to provide context for the type of impacts that might reasonably be considered within this event category. Because many, if not all, of these attacks did not produce national-level impacts, a second list of unintentional or non-cyber related failures within the critical

injury, followed by displacement. Uncertainty was captured by applying the index formula to the low, best, and high estimates of these three human impact metrics.

The Event Familiarity Factor is intended to capture the extent to which the event entails an ongoing threat with uncertainty regarding long term effects, is unfamiliar, or that people dread, exacerbating psychological impacts. This factor, ranging from 1.0 for familiar events to 1.3 for unfamiliar events, was provided by subject matter experts for each national-level event included in the SNRA: experts assessed a C_{EF} of 1.0 for the Cyber Event affecting Physical Infrastructure event.

As fatality and injury/illness estimates were not determined, psychological distress estimates could not be calculated for this event.

[12] The 2011 SNRA referred to impacts as 'consequences' because of prior usage in quantitative risk assessment (Kaplan and Garrick [1981, March], On the quantitative definition of risk: *Risk Analysis* 1(1) 11-32). Except where it will cause confusion, 'impact' is used synonymously in this document because of pre-existing connotations of the word 'consequence' within FEMA.

[13] See McAfee and the Center for Strategic and International Studies: 24.

infrastructure sectors is presented, in order to provide context on the potential magnitude of impacts produced by events in this category.

Targeted and Nontargeted Attacks on Critical Infrastructure Control Systems[14]
Worcester air traffic communications. In March 1997, a teenager in Worcester, Massachusetts, disabled part of the telephone network using a dial-up modem connected to the system. This disabled phone service to the airport control tower, airport security, the airport fire department, the weather service, and the carriers that use the airport. Also, the tower's main radio transmitter and another transmitter that activates runway lights were shut down, as well as a printer that controllers use to monitor flight progress. The attack also disrupted phone service to 600 homes in a nearby town.
Maroochy Shire sewage spill. In the spring of 2000, a former employee of an Australian organization that develops manufacturing software applied for a job with the local government, but was rejected. Over a 2-month period, this individual reportedly used a radio transmitter on as many as 46 occasions to remotely break into the controls of a sewage treatment system. He altered electronic data for particular sewerage pumping stations and caused malfunctions in their operations, ultimately releasing about 264,000 gallons of raw sewage into nearby rivers and parks.
Los Angeles traffic lights. According to several published reports, in August 2006, two Los Angeles city employees hacked into computers controlling the city's traffic lights and disrupted signal lights at four intersections, causing substantial backups and delays. The attacks were launched prior to an anticipated labor protest by the employees.
CSX train signaling system. In August 2003, the Sobig computer virus was blamed for shutting down train signaling systems throughout the East Coast of the United States. The virus infected the computer system at CSX Corporation's Jacksonville, Florida, headquarters, shutting down signaling, dispatching, and other systems. According to an Amtrak spokesman, 10 Amtrak trains were affected. Train service was either shut down or delayed up to 6 hours.
Davis-Besse power plant. The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again.
Zotob worm. In August 2005, a round of Internet worm infections knocked 13 of DaimlerChrysler's U.S. automobile manufacturing plants offline for almost an hour, leaving workers idle as infected Microsoft Windows systems were patched. Zotob and its variations also caused computer outages at heavy-equipment maker Caterpillar Inc., aircraft maker Boeing, and several large U.S. news organizations.
Harrisburg, Pennsylvania, water system. In October 2006, a foreign hacker penetrated security at a water filtering plant. The intruder planted malicious software that was capable of affecting the plant's water treatment operations. The infection occurred through the Internet and did not seem to be an attack that directly targeted the control system.
Lodz, Poland, tram system. In early 2008, a 14-year old boy jerry-rigged an infrared transmitter that allowed him to hack into the switching network of the Lodz, Poland, city tram system and cause four trams to derail, injuring at least a dozen riders.
Siberian hydro-electric plant. In Russia in the summer of 2009, maintenance personnel for a Siberian hydro-electric plant remotely logged on to the plant's control network and set the turbines to operate beyond safe parameters. One of the turbines was ejected from its moorings damaging additional turbines, leading to the generator room being flooded and causing a transformer explosion. The turbine room was destroyed and 75 workers were killed.

[14] The first seven entries in this table are quoted in whole from Government Accountability Office, Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain (September 2007): 15–17.

The Potential Magnitude of Critical Infrastructure Failures[15,16] (provided for context to encourage participants to consider potential consequences of a cyber attack)
Northeast power blackout. In August 2003, failure of the alarm processor in the control system of FirstEnergy, an Ohio-based electric utility, prevented control room operators from having adequate situational awareness of critical operational changes to the electrical grid. This problem was compounded when the state estimating program at the Midwest Independent System Operator failed due to incomplete information on the electric grid. When several key transmission lines in northern Ohio tripped due to contact with trees, they initiated a cascading failure of 508 generating units at 265 power plants across eight states and a Canadian province.
Taum Sauk Water Storage Dam failure. In December 2005, the Taum Sauk Water Storage Dam, approximately 100 miles south of St. Louis, Missouri, suffered a catastrophic failure, releasing a billion gallons of water. According to the dam's operator, the incident may have occurred because the gauges at the dam read differently than the gauges at the dam's remote monitoring station.
Bellingham, Washington, gasoline pipeline failure. In June 1999, 237,000 gallons of gasoline leaked from a 16-inch pipeline and ignited an hour and a half later, causing three deaths, eight injuries, and extensive property damage. The pipeline failure was exacerbated by poorly performing control systems that limited the ability of the pipeline controllers to see and react to the situation.
Browns Ferry power plant. In August 2006, two circulation pumps at Unit 3 of the Browns Ferry, Alabama, nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.

Additional References

Clem et al (2003). Health implications of cyber-terrorism. *Prehospital and Disaster Medicine* 18(3) 272-275.

Congressional Research Service (2007, January 22). Terrorist capabilities for cyberattack: overview and policy issues. CRS Report to Congress RL33123, Congressional Research Service, Library of Congress; at http://www.fas.org/sgp/crs/terror/RL33123.pdf (checked April 2013).

Lewis, James A. (2002, December). Assessing the risks of cyber terrorism, cyber war and other cyber threats. Center for Strategic and International Studies; at http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (checked April 2013).

Lewis, James A. (2010, March). The electrical grid as a target for cyber attack. Center for Strategic and International Studies; at http://csis.org/files/publication/100322_ElectricalGridAsATargetforCyberAttack.pdf (checked April 2013).

Lewis, James A (2011). Cybersecurity: assessing the immediate threat to the United States. Statement before the House Oversight and Government Reform Committee, Subcommittee on National Security, Homeland Defense, and Foreign Operations, May 25, 2011. Center for Strategic & International Studies (CSIS); at http://csis.org/testimony/cybersecurity-assessing-immediate-threat-united-states (checked April 2013).

Lewis, James A (2011). Examining the Cyber Threat to Critical Infrastructure and the American Economy. Statement before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, March 16, 2011. Center for Strategic & International Studies (CSIS); at http://csis.org/testimony/examining-cyber-threat-critical-infrastructure-and-american-economy (checked April 2013).

McAfee and the Center for Strategic and International Studies (April 2011). In the Dark: Critical Industries Confront Cyberattacks [McAfee second annual critical infrastructure protection report]; at http://www.mcafee.com/cip_report (checked April 2013).

McConnell, Mike (2011). Cyber insecurities: the 21st century threatscape. In Kahn et al, America's Cyber Future: Security and Prosperity in the Information Age (Chapter II). Center for a New American Security, May 31, 2011.

McGraw, Gary, Nathaniel Fick (2011). Separating threat from the hype: what Washington needs to know about cyber security. In Kahn et al, America's Cyber Future: Security and Prosperity in the Information Age (Chapter III). Center for a New American Security, May 31, 2011.

Nye, Joseph S, Jr. (2011). Power and national security in cyberspace. In Kahn et al, America's Cyber Future: Security and Prosperity in the Information Age (Chapter I). Center for a New American Security, May 31, 2011.

[15] This list was provided to the participants in the frequency elicitation, to encourage consideration of potential impacts of a cyber attack against physical infrastructure.
[16] The entries in this table are quoted in whole from Government Accountability Office: 16–17.

Organization for Economic Co-operation and Development (OECD) (2011, January 14). Reducing systemic cybersecurity risk. Report IFP/WKP/FGS(2011)2, OECD/International Futures Programme (IFP) Project on "Future Global Shocks"; at http://www.oecd.org/dataoecd/57/44/46889922.pdf (checked April 2013).

Schroeder, Christopher M. (2011). The unprecedented economic risks of network insecurity. In Kahn et al, America's Cyber Future: Security and Prosperity in the Information Age (Chapter X). Center for a New American Security, May 31, 2011.

Sumner, Mary (2009, January). Information security threats: a comparative analysis of impact, probability, and preparedness. *Information Systems Management* 26(1) 2-12.

U.S. Department of Homeland Security (2011, August). Information Technology Sector Baseline Risk Assessment; at http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf (checked April 2013)

Appendix L: Data Sources in the Classified SNRA

Blue text indicates superseded information.

The 2011 SNRA natural hazard and technological hazard data was derived completely from unclassified data, with substantial reliance on historical records. Data within the assessment which addresses only natural hazards and technological hazards has been treated as unclassified. The following paragraphs describe the derivation of the For Official Use Only and classified SNRA data which may be found in the classified SNRA Technical Report.

Impacts

For the adversarial/human-caused events, some impact estimates were unclassified but marked For Official Use Only (U//FOUO) in accordance with DHS practice, while other impact estimates were classified by derivation.

- For the conventional attack events (Armed Assault, Explosives, and Aircraft as a Weapon) fatality and injury/illness estimates were derived from unclassified historical data, as detailed in the corresponding risk summary sheets (Appendix J, SNRA 2011 Unclassified Documentation of Findings).[1] Following DHS practice these estimates were marked as (U//FOUO). Direct economic impact estimates were calculated from (U//FOUO) models and data using the Risk Assessment Process for Informed Decision-Making (RAPID) engine.[2]
- Fatality, injury/illness, and economic impact data for the CBRN events were uniformly obtained from the DHS Directorate of Science & Technology (S&T) 2011 Integrated Terrorism Risk Assessment (ITRA). While these estimates are unclassified in their original form, the CBRN data provided by S&T to the SNRA team utilized weighted average consequences, which incorporate frequencies (the modelled relative likelihood that an attack, given occurrence, will result in consequences of a given magnitude). This calculation elevated the CBRN impact estimates provided to the SNRA project to the SECRET//NOFORN classification level of the incorporated frequency data.
- Quantitative impact data for the cyber attack events were not determined. Although the 2011 project successfully elicited quantitative frequency estimates from Intelligence Community and DHS cyber experts (see below), these experts could not reach agreement on the consequences of attacks corresponding to the estimated frequencies. The 2015 SNRA qualitatively identified a broader taxonomy of cyber events, but did not attempt to determine quantitative impact estimates.[3]

Social displacement and environmental impact estimates were unclassified for all events.

[1] The primary sources for the Aircraft as a Weapon historical fatality and injury data are the same as those in the present volume, with minor differences. The primary historical data source for the 2011 Armed Assault and Explosives Terrorism Attack events was the START Global Terrorism Database, retained as a supplementary data source for the 2015 risk summary sheets.

[2] The Risk Assessment Process for Informed Decision Making (RAPID) 2010 was a strategic level, DHS-wide process to assess risk and inform strategic planning priorities developed by the DHS Office of Risk Management & Analysis (National Protection & Programs Directorate). The RAPID engine is a suite of computational tools for calculating human and economic measures of risk and the relative effectiveness of different DHS programs in risk reduction. Like the SNRA it is a quantitative tool for calculating and comparing risks in the homeland security mission space with each other, but unlike the SNRA it is designed for additionally calculating the comparative effectiveness of different governmental programs in buying down risk.

[3] The 2015 SNRA did not attempt to elicit updated frequency estimates. Although the 2011 qualitative cyber attack risk summary sheets are included in this volume for completeness, the corresponding frequency estimates are no longer current because of the substantial evolution of the cyber risk environment since 2011.

Frequency

Quantitative estimates of the frequency with which an adversarial/human-caused attack may be initiated and successfully executed were used as measures of the likelihood of SNRA events. Where subject matter expert judgment was used to determine frequency of successful attacks, adversary intent and capability were considered implicitly by the experts, but were not explicitly quantified or characterized. Attack initiations may occur with higher frequency than the ranges provided.

Due to the short timeline imposed by the PPD-8 Implementation Plan, the 2011 SNRA project team made a concerted effort to rely on previously conducted analyses wherever possible. Appropriate prior analysis had been accomplished for the CBRN, aircraft-as-a-weapon, and explosives terrorism attack events. For these events, all frequency and impact data derive directly from previously conducted analysis. The 2011 project team conducted expert elicitations for the armed assault and cyber attack events which had not been previously studied within a methodology comparable to the SNRA.

Existing Frequency Data

A designated Intelligence Community (IC) agency reviewed and commented on the relative frequency of the adversarial/human-caused events for which data was derived from previous governmental risk assessments, including DHS/S&T's Integrated Terrorism Risk Assessment (ITRA) and DHS/NPPD/RMA's Risk Assessment Process for Informed Decision-making (RAPID). To accomplish this, the agency reviewed frequency data, including the 5th, mean, and 95th percentiles of the frequency distributions. The review was performed in the summer of 2011. The IC agency did not comment on the absolute values of the frequencies.[4]

Elicited Frequency Data

Within the adversarial/human-caused set of events, there were two event types, armed assault and cyber (affecting data and affecting physical infrastructure) for which appropriate frequency data sources could not be located. For these events, an elicitation protocol was developed and separate elicitations were conducted of IC experts.

For the cyber elicitation, representatives from DHS/NPPD/CS&C, ODNI, CIA, FBI, NSS, and NSA participated in a two part elicitation. All participants attended a half day working session to discuss the scope of the cyber events, identify event thresholds, and begin to provide frequency data. A subset of the participating agencies (ODNI, CIA, FBI, NSS) then completed the frequency elicitation tool and submitted it as input for consideration and review by the larger group.

- Elicitations for the cyber attack against data incorporated three specific target types (financial institution system, public health/emergency system, internet) and asked that the elicitees provide individual frequency judgments for each of these target types.
- Elicitations for the cyber attack against physical infrastructure incorporated five specified target types (dam failure, chemical release, electric grid failure, radiological release from a nuclear reactor, transportation system failure) and asked that the elicitees provide individual frequency judgments.

[4] The IC agency did not comment on the relative ordering of the frequencies for the two cyber events or armed assault, since those frequencies had not yet been elicited from the Intelligence Community SMEs within the SNRA project's structured elicitation process.

- As noted above, no consensus consequence estimates corresponding to these elicited frequency judgments were obtained for the cyber events.

For the armed assault elicitation, representatives from DHS/I&A, FBI, and NSS participated in a group elicitation. All participants attended a half day working session to discuss the scope of the armed assault event, identify event thresholds, and provide frequency data. All data was collected during this group session, with the exception of one domestic terrorism expert who was individually elicited to ensure that domestic terrorism perspectives were included. No specific target types were articulated by the group.

For all elicitations, elicitees were asked to assign a frequency range to the events leveraging structured bins. Elicitees identified whether the frequency of these events were more or less frequent than once per year. If more frequent, elicitees then assigned the events to one of four buckets, each of varying order of magnitude (1-10 events per year, 11-100 events per year, 101-400 events per year, or greater than 400 events per year). If less frequent than once per year, elicitees assigned the events to one of four probability ranges (1% or less probable per year, 10% probable per year, 25% probable per year, or 50% probable per year). Elicitee input was aggregated into a range, which is represented within the SNRA frequency data.

Detail

Five SNRA adversarial/human-caused events are discussed as a unit below because the data within the SNRA was uniformly obtained from the DHS/ Science & Technology (S&T) 2011 Integrated Terrorism Risk Assessment (ITRA).

SNRA Chemical, Biological, Radiological, and Nuclear Terrorism Attack Events

Events Covered

- Biological Terrorism Attack (non-food)
- Chemical/Biological Food Contamination Terrorism Attack
- Chemical Terrorism Attack (non-food)
- Nuclear Terrorism Attack
- Radiological Terrorism Attack

Data Source

DHS/Science & Technology (S&T) 2011 Integrated Terrorism Risk Assessment (ITRA)

Data Gathering Process[5]

The Integrated CBRN Terrorism Risk Assessment elicitations were conducted throughout May and June 2010. Experts were formally elicited on five topics: absolute frequency of CBR initiation, relative frequency of CBR selection, absolute frequency of IND acquisition, frequency of CBRN interdictions, and CTRA and BTRA terrorist organization category capabilities. From this data, absolute frequency of acquisition for CBRN and the absolute frequency of attack with CBRN were calculated. Elicitation methods used were based on the approach described in NUREG-1150.[6] Elicitation experts followed the below steps in obtaining probabilities from intelligence analysts:

1. Pre-elicitation meeting: The group discussed the purpose and approach and scope of the planned elicitations
2. Intelink Terrorism Risk Assessment Frequency of Initiation Intellipedia discussion: Elicitees continued on-line discussion of event definitions and scope, to ensure shared definitions
3. Dissemination of elicitation materials: Elicitation materials were shared electronically to allow the group to review the elicitation process and event definitions
4. Study period/individual formal elicitation meetings: Individual elicitations were conducted
5. Group review meeting: The full panel reviewed the final results and confirmed or updated responses
6. Dissemination of group review meeting follow-up document and reconciliation responses: The final results were circulated amongst the group for documentation purposes

Resultant probabilities were based on analysts' knowledge of the field and prior exposure to intelligence reporting, but probabilities were not expressly linked to specific reporting. Probability distributions resulting from the elicitations were classified as SECRET//NOFORN.

Participating Organizations

A combined panel of CBRN experts was convened for elicitation purposes, including analysts from:

- National Counterterrorism Center
- Defense Intelligence Agency
- National Security Agency
- Office of the Director of National Intelligence (ODNI)
- DHS Office of Intelligence & Analysis

Experts who were selected generally had significant expertise in at least one of the four CBRN terrorism threat areas, along with knowledge of the other threat areas.

[5] This process description is a summation of material contained in the DHS Science & Technology Directorate's 2011 Integrated CBRN Terrorism Risk Assessment, Chapter 3: Technical Approach (p. 3-149 – 3-155). (Reference is SECRET//NOFORN; Extracted information is UNCLASSIFIED.)

[6] NUREG-1150 is an elicitation methodology developed by the Nuclear Regulatory Commission (NRC) in 1991 to formalize the process by which subject matter experts may provide probabilistic assessments in areas where data is sparse.

Two of the adversarial/human-caused events had previously been assessed within the DHS National Protection and Programs Directorate's (NPPD) Risk Assessment Process for Informed Decision-making (RAPID), which provided a quantitative assessment of strategic risk facing the Nation. These events are discussed as a unit below.

SNRA Explosives and Aircraft-as-a-Weapon Events
Events Covered • Explosives Terrorism Attack • Aircraft as a Weapon
Data Source NPPD RAPID (2010)
Data Gathering Process The RAPID elicitations were conducted between October 2009 and January 2010. Eleven experts participated in the elicitation process. Following a modified NUREG-1150 expert elicitation process, RAPID II was able to obtain likelihood probabilities for the terrorism incident sets. Elicitation experts followed the below steps in obtaining probabilities from intelligence analysts: 1. Identification of issues: Elicitation topics were identified in alignment with the analytic fault trees provided 2. Selection of experts: RAPID team members identified appropriate experts within the intelligence community 3. Individual elicitations performed: Using R Project, the RAPID team worked with experts to interactively create probability distributions which represent the likelihood that an adversary will initiate an attack, and, if initiated, the relative likelihood of different types of attacks 4. Review by experts: Experts reviewed anonymous inputs of all participating experts, with the opportunity to make adjustments The resultant probability distributions identified the likelihood with which particular attack types would be initiated and the likelihood that a particular target class would be selected. Resultant probabilities were based on analysts' knowledge of the field and prior exposure to intelligence reporting, but probabilities were not expressly linked to specific reporting. Probability distributions resulting from the elicitations were classified as SECRET//NOFORN.
Participating Organizations All eleven experts were from the DHS Office of Intelligence & Analysis (I&A) or a DHS operational component. Experts were selected based on their knowledge of the research area.

Finally, the SNRA team conducted original subject matter elicitations for two adversarial/ human-caused events. These elicitations were conducted separately but are treated as a unit here because the same elicitation protocol was used.

SNRA Armed Assault and Cyber Events

Events Covered

- Armed Assault
- Cyber Attack against Data
- Cyber Attack against Physical Infrastructure

Data Source

Original frequency elicitations conducted in August 2011 to support the SNRA

Data Gathering Process

Following a modified NUREG-1150 expert elicitation process, SNRA was able to obtain likelihood probabilities for the terrorism incident sets. Elicitation experts followed the below steps in obtaining probabilities from intelligence analysts:

1. Selection of experts: The SNRA team worked with staff within the ODNI to identify appropriate participants
2. Identification of issues: On the day of the elicitation, the experts discussed and agreed upon the definition of the events. Note that for cyber, the broad categories of attacks against data and attacks against physical systems had been previously constructed
3. Group elicitations performed: Using a binning structure, each member of the group provided their probability estimate. Some information was collected via an in-person group discussion, while some information was received in electronic form after the meeting
4. Review by experts: Following the elicitation, the SNRA team compiled the inputs and provided final outcomes to participants for review and comment

The resultant probability distributions identified the likelihood with which each event types would be initiated and the likelihood that a particular target class would be selected. Resultant probabilities were based on analysts' knowledge of the field and prior exposure to intelligence reporting, but probabilities were not expressly linked to specific reporting. Probability distributions resulting from the elicitations were classified as SECRET//NOFORN.

Participating Organizations

Armed Assault

- National Counterterrorism Center
- Department of Homeland Security Intelligence & Analysis
- Federal Bureau of Investigation

Cyber Attacks (Infrastructure and Data)

- Office of the Director for National Intelligence
- Central Intelligence Agency
- Federal Bureau of Investigation
- National Security Agency
- National Security Staff
- Department of Homeland Security Cyber Security and Communications

Derivative Classification Sources for SNRA Data

The following references are derivative classification sources for the classified data of the SNRA, as noted in the data tables provided in Appendices B through E of the classified SNRA Technical Report.

Armed Assault SME: Subject matter expert elicitation session with representatives from the DHS Office of Intelligence & Analysis (I&A), Federal Bureau of Investigation (FBI), and National Security Staff (NSS) (2011, July 26). Classification level of discussion was SECRET; Derived from: Multiple Sources; Declassify on: 20360726.

Cyber SME: Subject matter expert elicitation session with representatives from DHS National Protection and Programs Directorate Office of Cyber Security and Communications (CS&C), Office of the Director of National Intelligence (ODNI), Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), National Security Staff (NSS), and National Security Agency (NSA) (2011, July 25). Classification level of discussion was SECRET; Derived from: Multiple Sources; Declassify on: 20360725.

ITRA: Email correspondence from Program Manager, Integrated CBRN Terrorism Risk Assessment (ITRA), DHS Science & Technology Directorate (2011, September 28). Data file: '(SNF) 20110926 Uncertainty (U).zip'. Extracted information is SECRET//NOFORN; Derived from: Multiple Sources; Declassify on: 25X2.

ITRA – Nuclear Econ Update: Email correspondence from Battelle Memorial Institute Support Contractor, Integrated CBRN Terrorism Risk Assessment (ITRA) Program, DHS Science & Technology Directorate (2012, July 20). Data file: '(U) Histogram Bins Rad and Bio_files are SNF.zip'. Extracted information is SECRET//NOFORN; Derived from: Multiple Sources; Declassify on: 20370720.

RAPID: DHS Office of Risk Management & Analysis (RMA) Risk Assessment Process for Informed Decision-making (RAPID) Database. Accessed July 12, 2011. Extracted information is SECRET//NOFORN; Derived from: Multiple Sources; Declassify on: 20360712.

Additional detail is given in Appendix I of the classified SNRA Technical Report. Derivative classifications for narrative statements are noted as footnotes in the body of the classified SNRA Technical Report.