Cyber-Risk Scoping Study for the Strategic National Risk Assessment

Summary

The Office of Cyber and Infrastructure Analysis (OCIA) in the National Protection and Programs Directorate (NPPD) has worked with partners in NPPD to identify, scope, and provide preliminary assessments of the leading categories of risk from cybersecurity incidents, from 2015 and 2020.[464] While, this analysis is not definitive, it provides the first known assessment of such risks that is entirely unclassified and is not focused on vulnerabilities or threat actors, but on the consequences of such incidents on the victims of the attacks and the United States. This study will inform the update of the Strategic National Risk Assessment that is being refreshed as part of the National Preparedness Goal led by the Federal Emergency Management Agency (FEMA).

The February 2015 Worldwide Threat Assessment by the Office of the Director of National Intelligence (ODNI) summarizes the current state of affairs from a strategic perspective:

> Cyber-threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber-threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology (ICT) networks that support U.S. Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption. However, the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a "Cyber-Armageddon" scenario that debilitates the entire U.S. infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security. [465]

Both the ODNI and NPPD's assessments reveal that within the last few years there have been significant changes to the availability and transparency of information about cybersecurity concerns in the United States (U.S.) This development allows us to create an analytic product which provides qualitative assessments with quantitative details that illustrate the trends of increasing risks. The consequence-focus of this analysis shows that, while some scenarios create significant direct burdens on individual organizations, the overwhelming majority of the consequences are experienced broadly throughout the U.S. by individuals, companies, not-for-profit organizations, and government authorities at all levels. While some scenarios can be clearly associated with financial losses, other scenarios may have greater risk. Much of this risk-burden comes from the high degree of uncertainty.

[464] OCIA thanks U.S. Computer Emergency Readiness Team (US-CERT), Industrial Control Systems-Computer Emergency Readiness Team (ICS-CERT), the Office of Infrastructure Protection, private sector partners, and the NPPD Front Office for their contributions, as well as the many Whole of Community contributors to the SNRA.

[465] Clapper, James, Statement for the Record, Worldwide Threat Assessment of the Intelligence Community, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf , accessed March 24, 2015

Background

The body of evidence available to the public regarding cybersecurity incidents and their consequences is notoriously limited; information is revealed, rather than observed, and these revelations give us an incomplete view. Despite this challenge, NPPD believes that there is greater knowledge about cybersecurity risks today than there was when the first Strategic National Risk Assessment was conducted in 2011 to inform the National Preparedness Goal.

The distribution of this knowledge is inconsistent; it does not reflect the risk itself, so much as the degree to which victims of cybersecurity challenges have been forthcoming. We consider this analysis a scoping study, as it provides insights into size, depth, cost and frequency of various aspects of the risk space, without meeting a requirement to put forward comparable measures of expected loss for different types of scenarios. Furthermore, a scoping study also allows the use of inferred resources, which have greater uncertainty associated with them.

The selection of scenarios should help analysts and planners recognize general categories of risk in cyberspace and understand specific examples of how these incidents have developed. We hope that the readers who use this assessment will include those focused on:

- Proactive investments in improved information security,
- Proactive investments in operational alternatives that make an organization less vulnerable in the event of a cybersecurity incident,
- Preparations for responding to an incident that affects the data and operations of the organization, and
- Discussions and decisions about how to engage effectively in the public-private partnership necessary to understand and manage security and resilience risks.

These scenarios also allow the reader to gain insights into what is observed by NPPD, without having to delve into classified information or distorting our view of the cyber-risk landscape. The assessments for the scenario types may reflect publicly reported examples, insights from NPPD’s Industrial Control Systems Computer Emergency Response Team (ICS-CERT), analogy, or the results of simulations and analysis. The scenarios themselves reflect concerns identified by different stakeholders, including:

- State and local inputs in the Threat and Hazard Identification and Risk Assessment (THIRA), which showed a high level of concern with the uncertainty and poor preparedness for cybersecurity incidents. The raw data for the THIRA sometimes reflected inconsistencies or infeasibilities that we allowed in this study as a reflection of how unclear this threat space is, and we adjusted to generalized scenarios of types that allowed a productive assessment.
- Research of publically available reporting of incidents. Often, such research discovers instances of reported breaches or hints of problems that are not publically discussed. Not all data is presented consistently or disaggregated sufficiently so that one can discern the characteristics of individual cybersecurity incidents. Such research clearly reveals the degree to which there is little consensus for how to assess the consequences of such events.
- Reporting in the ICS-CERT Monitor. These scenarios reflect anonymized reporting by partners and may provide a clear basis for why stakeholders are so concerned about cybersecurity risks that have not really fully materialized.

- Scenarios developed for exercises by the National Cybersecurity and Communications Integration Center (NCCIC) that represent shared concerns among key partners. Exercises allowed them to discuss how partners would deal with a challenge as it emerges. Unlike the state and local-generated scenarios, the information and data available to the NCCIC reflects a much clearer understanding of cybersecurity professionals about how such incidents might unfold. They also reflected a general lack of understanding of how to assess the consequences.
- Office of Cyber and Infrastructure Analysis (OCIA)-identified scenarios. Such scenarios were developed when we found a category of cybersecurity incident that was sufficiently well defined that analysis could improve the body of knowledge and understanding about the potential risks. In some cases, OCIA used simple logic models to clarify how the results of an as yet unseen cyberattack would be analogous to the effects of another type of event. It is certain that the societal and economic consequences could be greater than most of the consequence assessments presented here. But it is helpful for planners and analysts to think through the logic of how such events unfold.

This study focuses on the types of victims, what it costs them, and whether or not we as a nation should expect these losses to increase. Analysts in the cybersecurity environment may wish to study this and other referenced cybersecurity annual reports to gain better insights into how to prepare for such incidents, and hopefully, how to avoid them. This study should help all readers understand why we should manage these risks.

The summary of these scenarios includes the general category of the scenario type, some distinct manifestations that affect the risk, and NPPD’s view of the risk trend from 2015-2020. The risk trend is a reflection of the combination of:

- frequency of incidents;
- strength, speed, virulence, of attacks; and
- value or scope of expected consequences – or both.

In scoping expected consequences we considered the pattern of vulnerabilities, the information and communications technology effects, the infrastructure functional effects (if they exist), and whatever organizational and societal consequences can be described.

It is extremely difficult to parse out the perception of the risk from the real risk in cybersecurity incidents. Our investments in cybersecurity pay off in increasing awareness. The increasing willingness of victims to report what is going on is believed to be an accurate reflection of real increasing risk. Some of these incidents, however, are discoveries that have been at risk for some time, but did not know it.

Those areas of the cyber-risk landscape that seem most uncertain may be prioritized to develop new analytic capabilities, improve information sharing, and to improve risk management and emergency response. The areas that seem to have more compelling evidence may be priorities for connecting the dots between the cybersecurity source of the risk, the operational activities that are impacted, and the executive decisions to manage risk across the enterprise.

Table 15 summarizes different categories of scenarios considered in this analysis, providing a qualitative assessment of the risk trend. These scenario types are described more fully in the pages that follow.

Category	Scenario	Type #	Page	Risk Trend
National security (NS)	Insider threat takes advantage of information security assumptions to facilitate a compromise of U.S. National Security Information and international standing	NS-1	608	High, Increasing Slightly
	Sensitive but unclassified information is extracted by an adversary and used for intelligence	NS-2	609	Moderate, Increasing Significantly
	Cyberattack interferes with availability of traffic flowing from a civil-purpose data source to a national-defense user	NS-3	610	Unclear
	Supply chain corruptions result in hardware or software that has imbedded exploits to be triggered by time or a change in conditions	NS-4	611	Unclear
Data breach (DB): Financial services	Systemically important bank is subjected smokescreen DDoS campaigns and the extraction of customer PII and financial data	DB-1	615	High, Increasing Significantly
	Payment system infrastructure is hacked, enabling criminals to increase the value of payments and create fraudulent means to receive payments	DB-2	617	Moderate-High, Increasing Slightly
	Criminal hackers install malware in payment card systems for national retailer, extracting PII and financial information for customers over the course of several months. The information is sold on the black market	DB-3	618	Moderate
Other data breach (DB)	Data breach extracts PII and other information from a government entity or not-for-profit	DB-4	622 (merged scenario)	Moderate, Increasing Significantly
	Data breach extracts PII, financial information and personal health information from hospital or insurer	DB-5		Moderate-High, Increasing Significantly
	Data breach extracts intellectual property from innovative businesses or R&D center	DB-6	624	High, Increasing Significantly
Cyber extortion or terrorism (EX)	Victim's data is destroyed, encrypted, or the victim is extorted with the threat of loss of access to their data	EX-1	628	*(not assessed)*
	Victim's web-enabled communications are hijacked by the attacker, who uses it to convey their own message or embarrass authorities	EX-2	630	*(not assessed)*
	Just DDos: DDoS attack campaign that just impedes access	EX-3	631	Low, Increasing Slightly
Attacks on ICS (ICS)	Distributed campaign of attacks on natural gas pipeline system ICSs, timed to maximize the impacts on energy assurance	ICS-1	636	Unclear
	Cyberattack on ICSs in a drinking water systems result in contaminated water supply [and broken infrastructure]	ICS-2	638	Unclear
	Complex coordinated attack on the grid is conducted so as to maximize physical damage and power outage	ICS-3	642	Unclear
Cyber-9/11[466] (c9/11)	Complex coordinated attack on significant infrastructure resulting in catastrophic outcomes	C9/11-1	645	Unclear for utilities, High, Increasing for Financial Services
	Cyberattack leaves malware inserted in the control systems of many key infrastructures without further activation, such as is observed with an advanced, persistent threat	C9/11-2	647	Unclear

Table 15: Summary of Cyber-Risk Scenarios

[466] In most cases, when someone refers to a cyber-9/11 they are not connecting this to terrorism, but to the concept of a large-scale attack that has a broadly felt negative impact on the Nation and compels a change in the way that governments and individuals go about their business. Other references to this game-changing cataclysmic event have included "cyber-Pearl Harbor" and "cyber-Armageddon".

National Security Scenarios

Introduction

It is very difficult to estimate risk for national security scenarios. There are intangible but sometimes existential values involved, such as national sovereignty, our ability to defend our homeland and interests in the event of hostility, the confidence of our people – and other nations – in our Government and our economy.

The question of risk is commonly determined for natural hazards, accidents, and random criminal acts as a function of likelihood and consequence. The frequency for such incidents is typically easy to discern based on observation of past incidents. However, for national security incidents there is a potentially large and unmeasurable gap between what is actually going on, and what is observed. Efforts to estimate such frequencies by observation will undoubtedly undervalue the risk dramatically. Efforts to estimate the real frequency of such incidents will be speculation.

This challenge is exasperated by the ambiguity of how to define the scope of an information-security-centric national security incident. It may be a single act of unlawfully collecting classified information or transferring it to a foreign national. Should it be the prolonged efforts over an entire career of acting in the clandestine service of a foreign government? Do we define it as the discovery or legal resolution of an espionage case in which the use of information technology (IT) was a primary means? Is it carrying out any intelligence operation through information and communications technology which once demanded human intelligence agents? Are some cyberattacks by nation-states an attempt to divert attention from some more subtle actions? Do sophisticated threat actors prepare complex overwhelming cyberattacks with physical system effects to obscure our ability to detect and defend against a physical attack? Do they use such attacks to remind other nations of their power to retaliate if they are not given full rein in other spheres of international influence?

In defining the impact of a national security incident, the primary measure may be a change of vulnerability. Our exposure as a nation is greater. There is also a cost. How do we account for the loss of the value of significant investments made to protect our nation?

What about nation-states' use of large volumes of sensitive-but-unclassified data to develop intelligence about the U.S.? The U.S. legal system and the Information Security Oversight Office recognize the responsibility of the U.S. Government to protect aggregated unclassified information with a classification in some cases. This is the recommended action in cases where the aggregate produces insights that warrant greater safeguarding of national security information. There is no mechanism to classify such information before it becomes aggregated, yet the use of modern cybersecurity exploits and Big Data analytic tools clearly enable foreign nations to develop the insights that our legal system expects us to protect as classified.

The lines between national security incidents and criminal acts become very blurred in cyberspace. When one considers the role of the foreign intelligence agents placed in the U.S. with false identities to function as spies and potential saboteurs during the Cold War, their assignments included tasks such as collecting information and preparing to disable the

Washington, D.C. electric grid and poison the public drinking water in the event of a superpower crisis.[467] The alignment of their tasks with the pattern of sophisticated cyberattacks on critical infrastructure-type targets suggests that the cyberattacks may be serving some of the same purposes as the sleeper cells of the Cold War. Like sleeper cells, advanced persistent threats (APTs) and sophisticated threat actors have historically been associated with highly resourced nation-states. They are able to gain access to computer systems and stay in these systems without detection for long periods of time. In some cases we have observed these types of attacks being brought to conclusion with extraordinary complexity in short periods of time. This is believed to be the result of the attackers' patient preparation of malware and exploits and readiness to wait for the timing to fulfill the objective of the attacker. The association of particular threats to any given nation is rarely publicly made. The ODNI reported that:

> Politically motivated attacks are now a growing reality with foreign actors reconnoitering and developing access to U.S. critical infrastructure systems which might be quickly exploited for disruption if the adversary's intent became hostile. In addition, those conducting cyber-espionage are targeting U.S Government, military, and commercial networks on a daily basis. These threats come from a range of actors, including: (1) nation states with highly sophisticated cyber programs (such as Russia or China), (2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea), (3) profit-motivated criminals, and (4) ideologically motivated hackers or extremists. Distinguishing between state and non-state actors within the same country is often difficult—especially when those varied actors actively collaborate, tacitly cooperate, condone criminal activity that only harms foreign victims, or utilize similar cyber-tools. [468]

This connection was made by the U.S. Department of Justice recently, in the indictment of a team of Chinese military hackers, and again when the Federal Bureau of Investigation (FBI) attributes the November 2014 Sony attack to North Korea. In the Worldwide Threat Assessment the ODNI highlights the growing number of computer forensic studies by industry experts that strongly suggest that several nations – including Iran and North Korea – have undertaken offensive cyber-operations against private sector targets to support their economic and foreign policy objectives, at times concurrent with political crises.[469] Despite these recent cases of attribution, it is generally very hard to make the connection between any particular attack and a particular nation-state or threat actor with great confidence.

Complicating this analysis is the fact that increasingly the nation-state actors and the criminal element are using the same methods and tools. The threat of destroying data or damaging infrastructure was used in the past by criminals to extort payment from owners and operators of critical infrastructure. The majority of infrastructure-focused incidents can be traced back to advanced, persistent threats or sophisticated threat actors and are not accompanied by demands for money. The perpetrators are simply in our systems…waiting, sometimes for years before

[467] Kalugin, Oleg, former KGB general, interviewed by Josh Rogin, for Foreignpolicy.com, *Ex-KGB general: Soviet sleeper agents were tasked with blowing up DC power grid; poisoning water supply*, http://foreignpolicy.com/2010/07/12/ex-kgb-general-soviet-sleeper-agents-were-tasked-with-blowing-up-dc-power-grid-poisoning-water-supply/ accessed March 4, 2015.
[468] Clapper, James, Worldwide Threat Assessment Report.
[469] Ibid.

they are discovered. Some national security-focused analysts give this a benign interpretation, seeing it as a present-day application of the theory of mutually assured destruction, which serves as a disincentive to nation-states to use powerful weapons and risk retaliation. Other analysts see this as a modern-day version of the Soviet illegals program[470]. Its secretive nature makes it less a disincentive, since it is not obvious, and more a contingency plan. The ODNI falls into this category, reporting that "Politically motivated cyberattacks are now a growing reality, and foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile.[471]

While the motivations of the individual nation-state intelligence services may be unknown, cyberattacks are affecting the civilian U.S. Government entities and the private sector and having a national security impact. Attacks that diminish the U.S. foundations of rule of law, respect for the privacy of the individual, intellectual property and economic security have the effect of degrading our national security. In most cases this is an indirect effect, thus, it is more subtle. This subtle erosion of our national values is difficult to manage because the victims cannot account for the idea that they are victims of well-planned foreign cyberattacks. We also have a hard time anticipating all of the systemic interdependencies among infrastructure sectors.[472]

Below is a small sample of the scenario space, each with a scoping assessment of the risk for the focus of the scenario. They are highly aggregated, limited by being completely unclassified, and by a lack of consensus for how to identify and measure the consequences. Scoping and contextualizing these risks is the first step to enable analysts to develop needed capabilities, for planners to begin to discern what response capabilities they lack, and to enable conversations about the value proposition for improving cybersecurity. Table 16 provides a more focused summary of the consequences, vulnerabilities and threats associated scenario 1. Subsequent tables will precede each scenario for the reader's convenience.

[470] The term "illegals" is used for intelligence staff officers who are recruited and trained to operate under deep cover in their target country. Unlike "legals" – intelligence officers who are given official diplomatic cover assignments and thus are protected by diplomatic immunity if discovered – illegals live and work seemingly ordinary lives, typically as immigrants with fake pasts. Illegals were expected to be ready to fulfill all manner of intelligence tasks when needed, from intelligence gathering to assassinations or sabotage, in the event of the outbreak of hostilities. For an article about this real, but rarely discussed practice, please see the Vanity Fair article, From Tradecraft to Sexpionage, Cold War K.G. B and U.S. Spies Concur: *The Americans* Actually Happened., http://www.vanityfair.com/hollywood/2014/05/the-americans-real accessed April 13, 2015

[471] Clapper, James, Worldwide Threat Assessment Report.

[472] Ibid. This point is made by the ODNI for some members of the private sector. NPPD believes this problem is more widespread.

Scenario	Consequences	Vulnerabilities	Threats
Insider threat takes advantage of information security assumptions to facilitate a compromise of U.S. National Security Information and international standing	The direct effects of these types of scenarios are the uncontrolled loss of classified information. The consequences, in peacetime include loss of value of intelligence sources and methods, loss of public trust, loss of international standing, competitive advantage to adversaries, and more. During a time of conflict these consequences could lead to unnecessary casualties, economic losses, and the risk of impaired national sovereignty.	Ineffective screening of personnel. Overly connected and unmonitored access to data within protected systems. Ability to use portable devices to collect records and to remove portable devices undetected.	Foreign intelligence agencies Unstable personnel in the cohort with unfettered access Disingenuous or corrupted individuals with unfettered access

Table 16: National Security Scenario Type 1

As information systems have become the core of the knowledge management and information sharing capability of the U.S. intelligence community, insider threats have increasingly used them as tools for collection and espionage. Since the year 2000, of the seventeen cases where a U.S. insider was accused or convicted of espionage in connection with their unlawful release of national security information, nine of those cases appear to have been facilitated by the use of computer systems in the furtherance of their crimes.

Some of these acts, most notably by Edward Snowden and Private Bradley Manning, took advantage of significant access to classified information systems to gather a broad range of information and used portable media to extract the data from its authorized location.[473]

A comparatively low consequence profile for such an incident would result from smaller amounts of less critical information being provided to a single adversary without a strong competitive advantage against the U.S. In cases where more information was carefully analyzed and prioritized for a highly capable foreign adversary's use, the consequences are much higher. Cases where individuals may have worked on behalf of Russia (or the former Soviet Union), accepted the protection of Russia, or who have pursued disclosure policies that benefit Russia are good examples of instances where there is greater harm. Examples of higher consequence cases that have harmed U.S. interests and international standing include the efforts of Robert Hanssen, Manning, and Snowden.[474]

The minimum economic consequences of such attacks are the exposure of significant U.S. sources and methods that cost at least tens of billions of U.S. dollars to develop and maintain.

[473] Edward Snowden was a contract computer professional who collected classified documents from the National Security Agency using his privileged access and then released portions of these documents publicly. Bradley Manning was an enlisted intelligence analyst in the U.S. Army who similarly collected classified documents and released them to the public through a website. Manning later underwent a gender transition and began using the name Chelsea.

[474] Robert Hanssen was an FBI agent who spied for the Russian Intelligence Services.

Exposing our sources and methods enables adversaries to develop ways to avoid being monitored, significantly reducing the value of the national investment. In the event of actual hostilities the strategic and operational value of this information is inestimable.

Analytic judgments of this situation, not guided by classified information, suggest that it is reasonable to project that such risks are increasing. From 2015 to 2020, given that current international tensions are becoming more acute and economic competition in the international marketplace plays an increasing role the past pattern of incidents is likely to continue. Individuals with authorized access are increasing the sophistication of their abuse of this access. The consequences of the public release or unauthorized transmittal to foreign agents of classified information may reasonably be greater, as the balance of power is shifting and tense. As our culture becomes increasingly fragmented and some in society view this type of activity as heroic, we might expect this to increase in frequency. However, this increase in motivated individuals may be counterbalanced by increasingly vigilant information security and counterintelligence.

Scenario	Consequences	Vulnerabilities	Threats
Sensitive but unclassified information is extracted by an adversary	Foreign intelligence services have large bodies of data useful for pattern analysis and future targeting. Often this is data about individuals with access to sensitive information.	Technical vulnerabilities vary. Management vulnerabilities include maintaining more PII, employment data, and other sensitive information than may be essential.	Foreign intelligence services conducting data breach attacks typically over the Internet

Table 17: National Security Scenario Type 2

Chinese intelligence efforts appear to take advantage of Big Data approaches to gathering unclassified information about individuals with access to classified information. Public reporting of the Anthem Blue Cross health insurance data breach attack revealed that there are strong indications the incident was perpetrated by Chinese hackers. Some have speculated about the value of the data on the large number of defense contractors at Northrup Grumman and Boeing whose personally identifiable information (PII) were gathered in the Anthem attack. [475] This attack will have serious economic repercussions on Anthem, and, if it is found to have exposed personal health information, it could theoretically cost the company over $800 billion, mostly in fines – which is likely to be an existential penalty. Limited regulatory tools meant to incentivize private companies to do all they can to safeguard individuals' data may also drive a wedge between the public and private sector in just such an area where collaboration is the only path to success. The more likely national security consequences of this attack may be that Chinese intelligence has large datasets that help them identify likely targets for further intelligence gathering.

Security researchers in Kaspersky Lab reported discovering a cyber-espionage campaign called "Careto", or "The Mask", which in February 2014 had been active in 31 countries for 7 years. The campaign appears to have been authored by Spanish attackers, and targets primarily

[475] Riley, Michael; Robertson, Jordan, Chinese State-Sponsored Hackers Suspected in Anthem Attack, http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack, accessed March 3, 2015

government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organizations and activists. Victims were in the Middle East and Europe to Africa and the Americas. [476]

It is possible that these attacks have a further destabilizing impact in the U.S. by creating incredible challenges for victim companies, who may believe they are using best known practices but are still successfully attacked. The 2015 Verizon Data Breach Investigations Report notes that "…the reality is that if a determined, state-sponsored adversary wants your data, they're going to get it unless another state-sponsored entity helps you defend it."[477] And yet, a political climate of distrust of companies and fear of new legislation or regulation establishes obstacles in the public-private partnership that must be engaged improve cybersecurity.

Attacks such as these that make use of large amounts of unclassified but sensitive data are likely to grow in frequency and sophistication over the next 5 years. The consequences of such attacks are likely to increase in two ways: the costs will increase for the direct victims (those experiencing the cybersecurity incidents), and the indirect victims (those whose personal information is being collected), and the U.S. will suffer a national security loss as adversaries gain valuable insights through the aggregation and abuse of sensitive but unclassified data.

Scenario	Consequences	Vulnerabilities	Threats
Cyberattack interferes with availability of traffic flowing from a civil-purpose source to a national-defense user	National defense utilizers of civil data become blind to a normal data input. In peacetime this may conceal an individual incident. During a time of conflict this may significantly empower an adversary.	Technical vulnerabilities vary, but are decreasing through proactive management.	Most likely foreign military intelligence services in support of tactical operations.

Table 18: National Security Scenario Type 3

Still other cyber-attacks can be designed to interfere with the normal movement of data that keeps our national defense authorities informed of the lawful movement of accepted civilian traffic, such as the Automated Identification System used by maritime vessels. This is a route-injection or route hijacking attack. A route injection or hijacking occurs when a threat actor gains access to routers running Border Gateway Protocol (BGP) and alters or injects their own route. Physical access is not necessary to exploit a vulnerability if the router can be found on the Internet. Filters are used to identify alternate data routes, but can be avoided by a savvy attacker. An incident such as this may obscure the situational awareness of defense authorities. Once detected, if the information flow is not restored, the detrimental outcomes are difficult to work around. It is not possible to replace a real-time data stream with snapshots and reporting by other

[476] Kaspersky Lab, Kaspersky Lab Uncovers "The Mask": One of the Most Advanced Global Cyberespionage Operations to Date Due to the Complexity of the Toolset Used by the Attackers, http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-Uncovers-The-Mask-One-of-the-Most-Advanced-Global-Cyber-espionage-Operations-to-Date-Due-to-the-Complexity-of-the-Toolset-Used-by-the-Attackers accessed March 17, 2015

[477] 2015 Data Breach Investigations Report, downloadable at http://www.verizonenterprise.com/DBIR/2015/?&keyword=p6922139254&gclid=CKb03ZXLisUCFbLm7AodFWQAqA, accessed April 22, 2015.

means, such as email and phone calls. During a time of peace, such a cybersecurity incident may be an impedance or nuisance, but it may provide a significant tactical advantage during hostility. A recent risk assessment completed in a coordinated effort between DHS and the Information Technology Sector, outlines more detail on risks to Domain Name Servers (DNS) and Internet routing. Specific to this scenario, they have identified areas of vulnerability targeted by threat actors and offer potential mitigations and recommendations with regards to risk management.

While the risk and the risk trends for scenarios such as this are unclear in this discussion, government analysts systematically try to discern scenarios that are effective for planning and proactive vulnerability management. The consequences of an attack such as this would likely be minor during peacetime, but significant during a time of crisis. They would be less for some types of civil-purposes, and greater for others. There is no basis to assess the frequency of attacks such as these, nor is frequency very relevant to the risk. In cases such as this, proactive management of the vulnerabilities is the commonly accepted approach.

Scenario	Consequences	Vulnerabilities	Threats
Supply chain corruptions result in hardware or software that has imbedded exploits to be triggered by time or a change in conditions	National defense agencies or defense contractors relying on software or hardware in sensitive systems lose access to reliable services when an exploit is triggered to execute an operation outside of the control of the system managers. During peacetime this may be mitigated by regular back-ups. During a time of conflict the loss of services may be timed to stress U.S. capacities just when they are needed.	Components or software manufactured or shipped through the control of adversaries	Foreign intelligence services controlling the operations or corrupt businesses seeking to profit by manufacturing counterfeit products without addressing known vulnerabilities.

Table 19: National Security Scenario Type 4

Analysts are concerned about the risks associated with supply chains. This includes the possibility that hardware or software may have originated in adversarial countries, or passed through adversary controls and now are corrupted with malware that may be activated at a later date. According to the CISCO 2014 Annual Security Report, "Malicious actors will seek out and exploit any security weakness in the technology supply chain. Vulnerabilities and intentional backdoors in technology products can ultimately provide them with access to the "full house." Backdoors have long been a security issue and should be a concern for organizations, because they exist solely to help facilitate surreptitious or criminal activity."[478] Even in networks that may have an excellent perimeter security, with no connectivity to the Internet, the possibility that data could be corrupted or destroyed within the network should remain a significant concern.

This concern has led to long collaboration among the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Defense Industrial Base Sector. Proactive action has resulted in a pilot program to mitigate supply chain risk for the defense industrial base, recognizing that it is typically their acquisitions that are tainted, rather than their production. This

[478] CISCO 2014 Annual Security Report http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf Accessed March 11, 2015

pilot is meant to deal with "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[479] The DOD pilot program will continue through FY 2017. It is not yet clear whether this pilot program will succeed in identifying and mitigating risks closer to the beginning of supply chains, or how successful it may be in light of the problem of counterfeit products entering the supply chain.

While this type of attack does not require a great deal of tactical sophistication to accomplish a great deal of harm, it does require knowledge of vulnerabilities along with logical or physical access, or both. When corrupted software or hardware makes its way to systems that connect to the Internet, it is possible that backdoors could be used later to trigger whatever harmful outcome is intended by an adversary. In systems without backdoors, adversaries could use a "set it and forget it" approach, which results in data destruction, or sabotage of a system when certain system parameters are reached. This latter scenario type, while feasible, is likely to be less appealing to adversaries as it removes so much active control. Supply chain vulnerabilities are greater in countries where manufacturing of counterfeit products is more common, or where governments legally require the collaboration of the private sector. Under such circumstances the challenges of coordination may be less of an obstacle than subject matter experts in the IT Sector assessed in the 2009 IT Sector Baseline Risk Assessment.[480] Their assessment that such attacks may be less frequent than other types of cyberattacks may be true, but the risks associated with tainted supply chains was sufficient for DHS's Office of Cybersecurity and Communications to establish an IT Supply Chain Risk Management program focused on addressing this challenge.

The effects of such attacks are simply that the adversary has accomplished a change of vulnerability. Instead of outside the fence, he is inside. The exploit that is triggered by any malware or further actions by an adversary is what would result in consequences, so they would greatly vary. The frequency of such attacks is unclear, but likely be less than common Internet-based attacks. This is a risk in which substantial efforts are now invested in controlling, and there are surprising discoveries of known vulnerabilities in newly acquired software. The efforts face greater challenges, however, in that it is difficult to find an unknown threat or vulnerability.

Financial Information and Other Data Breaches

Introduction

Financial-information-related cyberattacks have great value to both criminals as well as other adversaries. The increasing use of exploits that allow criminals to gather individuals' personal identity information (PII) and their financial information has demonstrated that this is a growing industry. This information can be sold on the black market or turned around by a multidisciplinary criminal organization to create counterfeit credit or debit cards and used as quickly as possible, to get as much cash as they can before the fraud is discovered. This endeavor easily brings in millions of dollars a year to individual criminal groups, with relatively low risk.

[479] Defense Federal Acquisition Regulation Supplement: Requirements Relating to Supply Chain Risk (DFARS Case 2012-D050) https://www.federalregister.gov/articles/2013/11/18/2013-27311/defense-federal-acquisition-regulation-supplement-requirements-relating-to-supply-chain-risk-dfars, accessed March 11, 2015

[480] IT Sector Baseline Risk Assessment, https://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf , accessed April 24, 2015

Data breaches that result in the loss of financial information are not unique to the Financial Services Sector. In fact, financial institutions are probably best equipped to deal with the losses, as they can recover their costs through their lines of business and their practice of covering the fraud losses of their customers has resulted in this being a fairly managed risk, from the perspective of the Sector. Nevertheless, identity theft remains the highest consumer complaint, according to the Federal Trade Commission, and harm from the exposure of an individual's PII is difficult to calculate.

The actual fraud loss going to the criminals is just one type of cost, as noted, typically covered by the financial institution if an institution is involved. In cases where retailers are also involved, the retailers themselves pay for services to protect their customers for a period of time as well. Other types of organizations also maintain individuals' PII and financial information, and it is much less clear what sort of resources they can use to provide comparable protections to individuals whose identities and financial information are compromised.

Furthermore, organizations may be fined, depending on what regulations apply to them, and their tolerance for absorbing these penalties may vary. Another source of loss is the direct costs of responding to cybersecurity incidents, which are going up as the complexity of attacks goes up and the level of defensive resources are invested in an attempt match it.

When one considers these as campaigns of recurring, high-frequency attacks, some with real direct fraud losses, fines, and most with increases in operational demand on defenders' information security and data centers, the costs of these attacks are becoming increasingly burdensome. In many cases the requirement for public notice is established by the State where the victims are found. A requirement to notify all whose identity is exposed results in significant additional costs for the victim organization, as the very act of dealing with the notification process is expensive, let alone the additional consequences the institution may take from the perspective of public confidence in the institution. Surveys by cybersecurity companies produce results too aggregated to assist in understanding risks for scenarios, but they do indicate that the costs of responding to cyberattacks is increasing dramatically, in part due to the increasing prevalence of using a distributed denial of service (DDoS) attack as a smokescreen to distract the cybersecurity staff while the criminals extract large volumes of data that they can then capitalize on. Forty percent of one survey's respondents reported losing more than $1 million a day from these sophisticated combination attacks.[481]

The concern about the level of cyberattacks against the U.S. financial services industry has increased significantly in the past few years. Information security threats prompted the Financial Stability Oversight Council in 2013 and 2014 to highlight operational risk, and information security in particular, as worthy of heightened risk management and supervisory attention.[482] In its 2014 annual report, the Council stated that mitigating evolving information security threats, effectively managing incidents, and promoting recovery efforts are critical to maintaining public confidence and reducing financial risk.

[481] Neustar, 2014 The Danger Deepens, Neustar Annual DDoS Attacks and Impact Report, http://www.neustar.biz/resources/whitepapers/ddos-protection/2014-annual-ddos-attacks-and-impact-report.pdf , accessed March 4, 2015

[482] The Financial Stability Oversight Council (FSOC) was established to identify risks to the financial stability of the United States, promote market discipline, and respond to emerging threats to the stability of the financial system. FSOC consists of 15 members, including the heads of the Department of the Treasury, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, National Credit Union Administration, and Securities and Exchange Commission.

The protection of critical infrastructure (which includes banking and financial institutions) from cyber threats is a high national priority, but different understandings of the Financial Services Sector leads to varied priorities among the different stakeholders. While the individual customer may be greatly concerned about identity theft and the possibility of becoming a victim of fraud, the institutions may view this risk as managed through their absorption of the fraud losses. National Sector leaders have a global view, informed by the comparison of the retail payment system, through which passes approximately $160 billion a day, to the wholesale payment system, through which passes $16 trillion a day. They encourage the institutions' effective management of these observed cybersecurity risks, while trying to assure the continued prevention of more catastrophic attacks against the Financial Services Sector infrastructure or those Communications Sector and Information Technology Sector infrastructures that they depend upon.

At least one important state regulator is concerned about the potential that banks may be unable to manage them, and, as a result, there may be cascading systemic risk that spills from one bank to affect others, and that this may in turn affect the larger economy. In a February 25, 2015 speech at Columbia Law School, Ben Lawsky, the Superintendent of New York's Department of Financial Services stated that he is concerned that there will be an attack on Wall Street firms that could "spill over into the broader economy." “We are concerned that within the next decade, or perhaps sooner, we will experience an Armageddon-type cyber event that causes a significant disruption in the financial system for a period of time," calling such an event a “cyber 9/11." If the changes that the New York Department of Financial Services proposes are put in place it will create new requirements for all of the Wall Street banks and insurers.[483] Since the majority of major financial institutions in the U.S. have a New York presence, this is significant.

There are many financial regulators at the Federal and state levels. In recent years as the global economy has become even more interdependent, the consensus guidance of international bodies of financial regulators has increased. Ultimately, the confusion and burden of many regulators creates an environment of distrust and a fear of being noncompliant. Compliance risk sometimes distracts organizations from other important risk management.

Simply reducing regulation is not necessarily the answer. Governments started regulating the financial services industry because of both criminal abuses and the realization that there are risks that emerge within markets or financial systems that propagate throughout the system of systems and into the larger economy. While activities that are highly regulated tend to be less profitable, which creates an incentive to innovate with new products, new payment platforms, etc., innovation is a mark of American strength. Today, within the financial services industry, much of these new innovations bring increasing exposure from cybersecurity risks.

Below are two scenarios which provide samples of this risk space. One highlights the potential for sudden and unexpected transitions to serious economic problems, the other highlights a risk that is becoming commonplace, expensive, and not always reported. There are many other scenarios that deserve assessment, but the potential consequences of these attacks can be so complex, and so fast moving that it is difficult to define and the available information for an assessment such as this is insufficient to provide value to planners. Such attacks may include

[483] Kaja Whitehouse, USA Today, Regulator warns of “Armageddon” cyber attacks on banks http://www.usatoday.com/story/money/business/2015/02/25/lawsky-goldman-sachs-banks/23995979/ accessed March 6, 2015

coordinated attacks on financial market utilities, securities or futures exchanges, etc. These scenarios may include attacks on the financial services infrastructure itself. The complexity of this sector, its increasing globalization, and its interconnection with current world events and individual perceptions make it difficult to develop a clear view of financial systemic risks.

Scenario	Consequences	Vulnerabilities	Threats
U.S. Systemically Important Bank is subjected to smokescreen DDoS campaigns and the extraction of customer personal identity information and financial data	Bank will absorb costs related to individual customers' initial credit monitoring and actual fraud, and costly incident management and notification activities. Additional soft costs relate to reputational risks for the bank, and substantial risk and time on the part of the customer, participating in the close monitoring of their credit and charges to their accounts, legal actions, and other uncovered expenses. If risks become intolerable and the public begins to distrust banks, problems for systemically important banks could have a destabilizing impact on the system of systems.	Interconnected systems allowing threat actors to infiltrate through smaller, less secure systems. Lack of oversight or management within organizations over newly installed technology and employees supporting.	Globally systemically important banks would logically be more likely targeted by criminals, terrorist groups, or agents of nation-states who are not well-integrated in the global economy. Risk of destabilizing the global economy is a disincentive to actors whose investments depend on financial stability.

Table 20: Data Breach Scenario Type 1

Systemically important banks (SIBs)are those banks that have met some threshold for heightened supervision based on the amount of assets they manage. Regulators are concerned that the role of these banks in the overarching financial system of systems is so great, that if some overwhelming stress impacts them and causes them to fail, the exposure of many other institutions to this failure could trigger another financial systemic risk event and potentially another global economic crisis such as was seen beginning in 2007. By requiring heightened supervision, related stress tests, greater capital reserves, and other risk management efforts to help them recover from their own incidents, rather than have a failure extend to others who are exposed to their problems, it is expected that the dominance of any one of these institutions will not lead to systemic reactions in the event that they experience shocks.

The international financial regulatory body, the Financial Stability Board, monitors and makes recommendations about the global financial system. The Board was responsible for identifying which banks fit into the category of Global Systemically Important Bank (G-SIB). Many, but not all of these banks are headquartered in the U.S. There is no evidence that cyber threats target these banks in an attempt to destabilize the global economy, just that their health is important to the global economy. The following G-SIBs are headquartered in the U.S.:

Global Systemically Important Banks Headquartered in the U.S.	
Bank of America	JP Morgan Chase
Bank of New York Mellon	Morgan Stanley
Citigroup	State Street
Goldman Sachs	Wells Fargo

An additional 24 G-SIBs are not headquartered in the U.S., though, by definition, the stability of these other banks is vital to the interests of the U.S. economy.

The Dodd-Frank Act established a threshold for any banks or bank holding companies that imposes heighted supervision standards. Any such institution with a balance sheet of greater than $50 billion is perceived in the international financial community as the equivalent of a U.S. domestically systemically important bank. Like the G-SIBs, there is no evidence that cyber threats are striving to destabilize the national or global economies through attacks on these banks. They are simply determined by legislated threshold to be of greater concern to avoid the potential that their failure may affect the larger economy.

U.S. Domestic Systemically Important Banks	
Ally Financial	KeyCorp
American Express	M&T Bank
BB&T	Northern Trust
BVA Compass	PNC Financial Services
BMO Financial Corp	RBS Citizens Financial Group
Capital One Financial	Regions Financial
Comerica	Santander Holdings USA
Discover Financial Services	Sun Trust Banks
Fifth Third Bank	U.S. Bancorp
HSBC North America Holdings	UnionBanCal
Huntington Bancshares	Zions

In a scenario of this type the target is a more capable defender, as it is one of the largest U.S. banks. The financial institution is hit with multiple campaigns of repeated DDoS attacks that serve as a smokescreen for data breach, which extracts customer financial information and PII. It is not uncommon that these attacks are so frequent that the victim bank has lost count; they are more than weekly. Some last for hours, others for several days. The institution must cover the losses of their customers, which they can recoup in part through fees and possibly insurance. They are very concerned about the hidden costs, such as the reputational risks, the churn of current customers going to other institutions and the potential that new customers would be put off from using their services in the future.

The Financial Stability Oversight Council's 2014 Annual Report contained at least six recommendations to stakeholders ranging from institutions to Congress for reducing cybersecurity risks. These recommendations include a demand for coordinated and collaborative Government-wide commitment and partnership with the private sector to promote infrastructure security and resilience, increased accountability through financial regulators of institutions' efforts to assess cyber-related vulnerabilities and to address gaps in oversight, increased engagement between institutions and private sector infrastructure cybersecurity providers, improved information sharing, and removal of legal barriers.

Banks have increased their investments in cybersecurity attempting to manage these risks yet they continue to experience them and incur additional costs. Occasionally, they have had to cover $5M-$10M real financial losses for customers who have become victims of fraud. They have observed that their shareholder value dips, but not for more than a few weeks. JP Morgan Chase announced plans, after experiencing the 2012 to 2013 DDoS attacks on the U.S. Financial

Services Sector, to increase their annual cybersecurity expenditures to $250 million by the end of 2014. After they suffered a hacking intrusion in 2014, JPMorgan's CEO said he would probably double JPMorgan's annual computer security budget within the next five years.[484]

The sophistication of these attacks is increasing, not just in terms of the combinations of cyber threats used in perpetrating the attacks, but with organization of teams of people ready to promptly make use of stolen financial information. The consequences are increasing as the sophistication increases, but there are additional risks that may emerge if a systemic reaction is triggered. The frequency of such attacks for individual institutions is expected to increase between 2015 and 2020 and the number of institutions affected is also likely to increase. We have no expectation that an adversary would attempt to induce a larger systemic risk that would impact the global economy, but there are often unintended consequences in highly complex interdependent systems, and the risk of systemic responses remains a concern.

Scenario	Consequences	Vulnerabilities	Threats
Retail Payment Service Provider is Hacked, Enabling Criminals to Increase the Value of Payments and Create Fraudulent Means to Receive Payments	Owners and operators of payment system infrastructure are apt to cover fraudulent payments and monitor the credit of impacted parties. Additional soft costs relate to reputational risk for the service provider, substantial risk and time on the part of customers and payees, participating in the close monitoring of charges to their accounts, evidence of identity fraud, legal actions, some of which is not covered by the payment service provider.	Lack of system awareness and understanding.	Criminal groups are most likely to attack payment service providers in an attempt to quickly siphon large amounts of funds.

Table 21: Data Breach Scenario Type 2

Payment infrastructure is complex and diverse, and innovations in how payments are made are sometimes better understood by international criminals than they are by many in the U.S. The feasibility of computer-enabled interference or manipulation of many of these systems is unclear. It is clear that some criminal hackers have figured out how to manipulate at least small portions of and turn it into a profitable criminal endeavor.

In one international hacking event that has been successfully prosecuted, a criminal group used sophisticated techniques to compromise the data encryption that was used by Royal Bank of Scotland's RBS WorldPay to protect customer data on payroll debit cards. Payroll debit cards are used by various companies to pay their employees. By using a payroll debit card, employees are able to withdraw their regular salaries from an ATM. Once in, the criminals raised the account limits on compromised accounts, and then provided a network of cashers with 44 counterfeit payroll debit cards, which were used to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the U.S., Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada. The $9 million loss occurred within a span of less than 12 hours.[485]

[484] Clapper, James, Worldwide Threat Assessment

[485] 2008 attack through payment infrastructure, with international collaboration. http://www.justice.gov/usao/gan/press/2014/10-24-14.html

Financial infrastructure systems are complex. This payment card system is not common in the U.S. In addition to understanding how to successfully execute a cyberattack, this criminal enterprise had to identify infrastructure elements that operate in the background, figure out how to manipulate them, and develop and manage teams around the world to quickly complete the crime. The sophistication of attacks on portions of the retail payment infrastructure is multidisciplinary, challenging, but likely to increase. It was remarkable that RBS WorldPay and international authorities were able to respond as well as they did. Criminal groups are likely to be working on new attacks. The consequences of such attacks are also likely to increase as the motives for improving the criminal endeavor is to get away with more money. The frequency of such attacks is likely to increase as well, as the incentives to do them are significant.

Scenario	Consequences	Vulnerabilities	Threats
Criminal Hackers Install Malware in Retail Payment Card Readers at a National Retail Chain	Here the costs are both economic and societal. Financial institutions and victims of identity theft shoulder the burdens with fines and recovery payments, along with the steps needed to rebuild and maintain credit.	Interconnected systems allowing threat actors to infiltrate through smaller, less secure systems. Lack of monitoring activities over legacy and newly installed technology.	Criminal hackers are the most likely threat actors.

Table 22: Data Breach Scenario Type 3

This portion of the retail payment system is part financial services and part commercial retail industry. Cybersecurity attacks here affect the card issuers, the retail chain, and of course, the customer. In this scenario type, criminal hackers install malware in retail payment card reader systems at a national chain, extracting PII and financial information for customers over the course of several months. The information is sold on the black market, and retailers and card issuers incur significant costs to compensate the affected customers, though the long-term impact for many customers remains significant. For some customers this impact is unnoticed or delayed; some criminals hold the stolen PII until the incident appears to have faded from public notice. Despite the fact that there are increasing notifications of these events, it is suspected that these events are now occurring without notice, as they are yet to be identified. Typically these crimes are discovered, by either actual fraudulent use of the customers' account details in online or telephone purchases that are challenged, or by the discovery of large amounts of customer PII and financial information for sale on the black market. A smaller percentage of these cyberattacks result in the quick manufacture of counterfeit physical payment cards.

There has been such an intense and broad set of cyberattacks against retailers in recent times that a multi-agency Government task force looked into these attacks to determine if there was evidence that they were a coordinated campaign designed to adversely affect the U.S. economy. In their two page report, the National Cyber Investigative Joint Task Force stated that they have not found evidence of overarching responsibility behind all of the attacks, but they underscored that the global implications of the retail attacks and the economic impacts to private business and individuals cannot be overstated.[486]

Numerous efforts have been made to account for the costs associated with such events. In addition to the costs that are reported in cybersecurity industry surveys about dealing with the expense of responding to cybersecurity incidents (too aggregated to be used here), the U.S. Sentencing Guidelines provides a useful estimate of the minimal costs associated with the loss of personal financial data that is sufficient to commit fraud. The intention behind the sentencing guidelines is not to estimate the actual financial losses that any individual company or affected customer experiences from the crime, but to provide a defensible approximation of the average combined costs for all stakeholders. Recent studies have suggested that any fixed cost per record is apt to produce an erroneous result.[487]

What are these costs? The company itself suddenly has to turn to corporate emergency response mode to address the incident, pay fines, fees, hire consultants, possibly notify victims, etc. It is the reputational costs, the opportunity costs of work that did not get done because of this attack, as well as churn that results as their customers go to competitors. In addition to these costs, many of the criminals turn around and use stolen identity information to file for tax refunds. The Internal Revenue Service (IRS) reported that, while they estimate that they prevented $24.2 billion in fraudulent identity refunds in 2013, they still paid out $5.8 billion in fraudulent refunds—and that is just what they know about.[488]

To a degree, individuals bear similar costs when they become victims of identity theft. Even if no actual fraud takes place, the victim often has to invest time and resources to address his or her risk. They may cancel cards and increase monitoring of their financial information. If the data is used and an individual becomes the victim of identity fraud, the individual may suffer much greater losses. While financial institutions bear the burden for those fraud losses that may be promptly realized, it is not hard to see that once someone's PII and financial information is out in the domain of criminals, the possibility of long lasting harm is quite real. The Federal Trade Commission estimated that identity theft takes an average of 200 hours of work and six months to recover. Most of this work involves keeping track of creditors, correspondence and phone calls, working with law enforcement and working with credit bureaus. These efforts are needed to prevent the victim from being liable for the debts the imposter created in their name, if actual fraud occurs. Additional work is needed in the fight to recover an accurate credit score. Since credit scores are used to establish the interest rates one is charged and whether or not credit will be offered, without this investment the victim will continue to pay for years. In some cases, victims of identity fraud lose out on job opportunities because they appear to be unreliable. Victims of identity theft choose to do all this work to restore the true record of their credit. It may be a better alternative to being held responsible for these debts, but it is a real cost to the individual. And yet, once individuals do most of the work to set up their own monitoring, the actual effort is not likely to increase much if their identity is stolen a second time. Thus, the

[486] Associated Press, U.S. retail cyberattacks not coordinated, shows government report, http://m.tech.firstpost.com/news-analysis/us-retail-cyberattacks-not-coordinated-shows-government-report-217998.html accessed March 17, 2014

[487] Verizon 2015 Data Breach Investigation Report, downloadable at http://www.verizonenterprise.com/DBIR/2015/ , accessed April 24, 2015

[488] Robert. W. Wood, IRS Paid $5.8 Billion in Fraudulent Refunds, Identity Theft Efforts Need Work, http://www.forbes.com/sites/robertwood/2015/02/19/irs-paid-5-8-billion-in-fraudulent-refunds-identity-theft-efforts-need-work/ accessed March 18, 2015

costs per record would logically go down for the individual, who may actually pass on lower costs per record to the institution that lost their data. How many credit monitoring efforts are needed?

The difference between identity theft and identity fraud is that a victim of identity theft may not experience the actual losses associated with the criminal using their data to commit fraud. Unfortunately, this distinction is not always clear in research and reporting on the topic; but this appears to be an important distinction. It reveals that the extraordinary work that both industry and individuals take on after identity theft occurs appears to be paying off. After a trend of increasing numbers of U.S. fraud cases from 2010 to 2013, the 2014 number of cases dropped 3 percent to 12.7 from 13.1 million cases in 2013. The total fraud losses dropped 11 percent to $16 billion, from $18 billion in 2013.[489] As both the number of cases drops and the total lost through fraud is calculated, however, it is important that to recognize that the amount of time and money spent by companies and individuals to prevent these losses is not included in the estimates. It remains a big problem.

In view of the information above, it is clear that these losses are not all borne by the retailers or the card issuers, nor can they easily be accounted for. There is some additional societal cost and individual harm. But it is not reasonable to just directly utilize these Sentencing Guidelines as a proxy for losses. They are explicitly about unauthorized telecommunication access devices, and, while it is clear that payment card skimming devices fall within the guidelines, it is not clear how the Sentencing Guidelines would apply to hacks that did not use a card skimmer. The Sentencing Guidelines have no clear reference to the number of victims or number of records of an incident. The financial estimates that refer to these Guidelines seem to interpret the illegal extraction of the electronic record as an instance of the use of an unauthorized access device, which this analysis can neither endorse nor dispute.

While those that argue against the use of the Sentencing Guidelines suggest that it inflates the cost, it could be argued that the Sentencing Guidelines may undervalue the losses. As written, if the unauthorized access device is unused (i.e. only identity theft), the minimal potential loss is $100 per affected account. If the data is used (i.e. unauthorized charges take place), the minimal potential loss goes up to $500 per affected account.[490] Thus, in addition to the costs accrued by the retailers and the card issuers for dealing with the cybersecurity incident itself, the minimal costs associated with the impact on the individual may be what is reflected in these loss estimates that refer to these Guidelines. If the Federal Trade Commission analysis is correct, the $100 for the average American’s 200 hours of work to clear up identity theft is clearly underestimating the harm.

The 2015 Verizon Data Breach Investigation Report has probably produced the most authoritative and understandable estimates of the insured costs for data breaches, through contributions from NetDiligence, which partners with cyber-insurance carriers to aggregate data on cyber liability insurance claims and produces its own *Cyber Liability and Data Breach Insurance Claims* study. Through this collaboration, Verizon was able to improve their loss

[489] Javelin Strategy and Research, https://www.javelinstrategy.com/news/1556/92/16-Billion-Stolen-from-12-7-Million-Identity-Fraud-Victims-in-2014-According-to-Javelin-Strategy-Research/d,pressRoomDetail, accessed March 18, 2015

[490] U.S. Sentencing Guidelines Manual, http://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2014/2B1.1.pdf, accessed February 24, 2015

estimation models and they realized that the cost of a data breach with a small number of records loss had a much higher per-record cost, whereas those breaches where an organization lost millions of records, had a much lower per-record cost. The evidence shows that the range of forecasted average costs for the same number of records still remains wide, typically more than an order of magnitude for the same number of records lost.

The Verizon model forecast that the average loss for a breach of 1,000 records would be between $52,000 and $87,000, with 95 percent confidence. The breach affecting 10 million records has an average loss forecasted between $2.1 million and $5.2 million. The confidence interval widens as the number of records increases to account for growing uncertainty. This means that the cost per record goes down as the number of records goes up, and the amount of uncertainty goes up as the number of records goes up.

This recent reporting reveals why it is wrong to try to rely on a single point estimate per record. Verizon concludes that the improvements to understanding this variation would probably be tied to collecting more and different data in order to make better models.[491] Some of the data that may explain the wide variations might include information about the cost as it relates to the organizations past experience with data breaches. If this is the first or the fifteenth data breach, we might expect that the institutional costs associated with dealing with the problem would reduce over time. Many other factors (type of organization, regulatory framework, etc.) may have an impact on costs beyond just the number of records.

In retail point-of-sale attacks that took place between 2013 and 2014 there were a number that made the news. On the lower end of the large data breach attacks, was the attack on Sally Beauty Supply, which affected just 282,000 customer cards. There were two attacks that affected less than a half million cards reported in 2014, and an additional three comparably sized retailers who did not report the number of cards affected.

There were two reported incidents in 2013–2014 where between a half million and a million customer records were affected. For example, the September 2014 Goodwill Industries attack exposed 868 thousand customers.

More alarming were the attacks on Harbor Freight (a tool vendor with 445 stores and nearly 200 million customers), Home Depot and Target. The number of compromised records for Harbor Freight is still unclear. Home Depot reported attacks that affected 56 million customers; they estimated their cost of the breach to be $62 million.

It is reasonable to expect that as the value of these attacks goes up for the criminals, they will become an attack vector of choice and more sophisticated. We would expect that, unchecked, these attacks will continue to increase significantly in scale and scope, consequences and frequency during the next 5 years. This estimate of increasing risk may need to be moderated, however. Recent efforts of retailers and card issuers to reduce the possibility of such attacks have lead them to become more adept at discovering these incidents quickly, thus stopping the losses sooner and reducing the number of customers exposed. Efforts to clearly notify customers whose identity has been stolen also help keep them from becoming the victims of fraud as well.

[491] Verizon 2015 Data Breach Investigations Report; downloadable at http://www.verizonenterprise.com/DBIR/2015/ accessed April 24, 2015

Data Breaches Complicated by Other Factors

Introduction

Outside of financial institutions and retail businesses there are other types of data breach scenarios that have discernibly different outcomes and consequences. Many state and local governments, universities, utilities, healthcare organizations and other entities use online customer service systems or maintain databases with personal and financial information to allow automatic billing and telephone or online payments. All of these organizations hold PII and financial information, but may not be expected (or able) to cover the losses of individuals who become the victims of identity theft or fraud to the same degree as financial institutions or retailers may be. Just as the requirement to notify victims varies among states, the responsibilities of different types of organizations vary greatly as well.

Scenario	Consequences	Vulnerabilities	Threats
Data breach extracts PII and other information from a government entity or not-for-profit, or health care entity	Consequences range from loss of PII to consumer confidence, not to mention the economic losses incurred by both the organization and the public.	Lack of adequate system protection, monitoring activities, and training of employees.	Criminal hackers are the most likely threat actors.

Table 23: Data Breach Scenario Type 4/5 (merged scenario)

When a commercial entity suffers from attacks that steal customers' PII and financial information they have some recourse and established processes to recoup these losses through fees and increases in prices. When a not-for-profit or government agency is subjected to the same attack, it is disproportionately painful. Summarizing the big victims in 2014, Advisen's Cyberrisk Network reported the U.S. Office of Personnel Management suffered such an attack in 2014, losing 5 million records, the U.S. Postal Service lost 3.7 million, and the Texas Health and Human Services Commission lost 2 million. By cost, the U.S. Marshals Service was found to have lost $18 million, the Oregon Department of Employment lost $16 million, and Miami-Dade county $3.3 million. The University of Maryland lost $2.6 million.[492] Goodwill Industries, noted earlier as a retailer subjected to a point-of-sale hack, as a not-for-profit has nowhere near the capability to absorb such losses as an ordinary retailer might.

In early 2015, the news of a significant attack on Anthem Blue Cross rolled out in pieces as the scope of the incident unfolded. At the time of this writing, Anthem reports that no individuals' personal health information has been compromised, but approximately 80 million current and former customers and employees of Anthem and other Blue Cross affiliates have had their PII and financial information stolen by the perpetrators.[493,494] Anthem is offering the same

[492] Josh Bradford, 2014 by the Numbers, Record-Setting Cyber Breaches, http://www.cyberrisknetwork.com/2014/12/31/2014-year-cyber-breaches/, accessed March 5, 2015
[493] http://www.cyberrisknetwork.com/2014/12/31/2014-year-cyber-breaches/
[494] Kaiser Health News, FBI Closing in on Culprits Behind Massive Cyberattack on Anthem's Database, http://kaiserhealthnews.org/morning-breakout/fbi-closing-in-on-culprits-behind-massive-cyberattack-on-anthems-database/ accessed March 5, 2015

protections of credit monitoring that retailers might under such circumstances. However, some analysts differ as to whether or not personal health information was compromised. If it is discovered that the data that was extracted included protected health information, in addition to the costs that Anthem is paying to deal with the incident, they will be required to pay penalties ranging from $100 – $50,000 for each violation up to $1,500,000 in a calendar year.[495] It is not yet clear how many calendar years may be in question.

While this scenario is very similar to other data breach scenarios, it is important to realize that the penalties for exposing personal health information are different and additional. The consequences of nearly the same incident seem to be greater when in involves healthcare information. The Symantec Internet Security Threat Report 2014 reported that Healthcare, Education and the Public Sector were ranked highest for the number of data breach incidents in 2013, accounting for 58 percent of all data breaches. However, these three sectors lagged way behind when viewed from the perspective of the numbers of identities exposed. The most lucrative way to steal identities is targeting retail, computer software, and financial institutions accounting for 77 percent of the identities exposed, compared to only 2.1 percent of the identities exposed through attacks on Healthcare, Education and the Public Sector.

Such data breaches experienced by the health care industry, not-for-profits, and government agencies may be increasing in scope, but not necessarily in sophistication. The outcomes of these attacks are not as obviously lucrative to the attacker. It is clearly more valuable to a criminal to target retailers or financial institutions, but the consequences of these attacks are different in many ways. Government agencies, education and not-for-profits are less able to invest in system protections, but even much less able to provide the same types of identity monitoring protections to individuals whose identities are exposed. Individuals may lose confidence these institutions, and not-for-profits may suffer greatly in consequence to such a loss. Agencies may also suffer from the loss of public trust, but it is not existential to them. Individuals cannot easily shift to a different agency because one of them failed to meet their expectations. Thus, while it may be more costly and difficult for a company to manage the consequences of a similar event and compensate the affected customers, it is possibly worse for individuals to feel helplessly dependent on an agency to protect their information and have no recourse when the protections fail.

[495] Ellen Tucker, Anthem Cyber Attack, The Importance of Data Security, http://blog.capital.org/anthem-cyber-attack-the-importance-of-data-security/, accessed March 5, 2015

Scenario	Consequences	Vulnerabilities	Threats
Data breach extracts intellectual property from innovative businesses or research and development center	The theft and/or destruction of intellectual property can set research and development within an organization back in their production, undermining pricing strategy and investment costs or takes them out of business.	Integrated systems that can be breached through lesser protected businesses. Lack of security (physical and/or logical), monitoring activities, and training of employees.	Criminal hackers, corporate espionage, and nation states interested in the intellectual property are the most likely threat actors.

Table 24: Data Breach Scenario Type 6

There are several examples of data breaches, including instances where intellectual property appear to be the target. There is no clear and commonly held method of evaluating the value of the loss of intellectual property. It is difficult to establish because there are so many competing issues involved. When someone steals a copy of intellectual property, the rightful owner still retains the use of this data. It still has some value to its rightful owner. Its value is greatly decreased if the theft results in a cheaper knock-off of their own product that undermines their pricing strategy in the market place. It could be even worse if every instance of the data in the rightful owners' databases is completely destroyed. When someone steals intellectual property, they do so because the thief recognizes that they will benefit from the results of the innovative research and development (R&D) that the victim has invested, potentially years' worth of work and in some industries, billions of dollars of effort. The pharmaceutical industry, for example, is noteworthy for having the legal right to have no other manufacturers use their formulation to produce generic drugs for twenty years, so that they can recoup their investments in R&D. In developing innovations, it is not just the time, effort and expense of creating something that works, but the cost associated with discovering what doesn't work that must be considered.

Assessments in this scenario type cannot have high confidence, because it is not common for victims to advertise their losses or for law enforcement to successfully identify and prosecute perpetrators of intellectual property theft. There have been numerous citations of large figures associated with the theft of intellectual property, most notably the 2013 estimate of over $300 billion dollars a year – the value of the U.S. exports to Asia.[496] But these estimates reflect an admittedly weak valuation capability, and they ultimately are tied back to the loss of all intellectual property in the U.S., including the manufacture of bootleg CDs, DVDs, designer purses and the like. Perhaps a more compelling consideration is the fact that, as cyberattacks by competitors or by foreign governments who provide the stolen data to their national industries continues, this loss of the value of their investment puts companies at risk of going out of business and costs the victim national economy significantly. As economic and political adversaries grow more sophisticated and confident in their ability to operate with impunity in U.S. networks, they are likely to recognize cyberattacks as a more efficient and effective way to

[496] The Report of the Commission on the Theft of American Intellectual Property, http://www.ipcommission.org/report/ip_commission_report_052213.pdf, accessed March 5, 2015.

get what they are after. Cyberattacks have become the dominant focus of experts in field of intellectual property theft.

This problem is greater now than it ever has been, in part due to the interconnectedness of our economic world. This is reflected in global supply chains, multinational corporations and the heavy reliance on the Internet. These factors make it easier to access the intellectual property of a competitor, without the cost involved in a corporate espionage effort.

According to a figure cited in the President's 2006 Economic Report to Congress, 70 percent of the value of publicly traded corporations is estimated to be in "intangible assets," that is, intellectual property. A 2012 study by the Department of Commerce found that protection and enforcement of intellectual property rights around the globe directly affects an estimated 27 million American jobs in intellectual-property-intensive industries, which is roughly 19 percent of the U.S. workforce, producing over one-third of America's GDP. [497]

The Commission on the Theft of American Intellectual Property noted that in addition to the direct losses felt by victims, if American intellectual property rights were respected overseas as they are here, the U.S. economy would add millions of jobs and restore incentives for innovation and investment, resulting in a significant growth to the U.S. gross domestic product. The U.S. Trade Representative's "2012 Special 301 Report" points out that while Ukraine, Russia and India contribute significantly to the volume of intellectual property theft from the U.S., 50–80 percent of our loss is to China.[498]

Both Verizon, a broadband and telecommunications company, and Mandiant, a cybersecurity firm have conducted studies that point to overwhelming responsibility for cyberattacks aimed at economic espionage being attributed to state-affiliated actors in the People's Republic of China (PRC). These assertions were endorsed by the U.S. DOD in its 2013 report to Congress on Chinese military developments. Reinforcing the findings from the Mandiant Corporation, their report notes that the PRC "is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs." It asserts that "the information targeted could potentially be used to benefit China's defense industry, high technology industries, [and] policymaker interest in U.S. leadership thinking on key China issues," among other things.[499]

It is because there is such strong consensus that there is a significant, under-discovered, under-reported and unmeasured risk associated with the loss of intellectual property through cyberattacks that the examples serve as exceptionally weak representations of the risks. Except in cases where victim organizations come forward publically to help prosecute criminals or draw attention to the issue, much of this is reported only confidentially, if at all.

Some cases help to clarify the scale of these losses, however. A single attack against RSA in 2011, the maker of the widely used SecurID tokens, which was traced back to China, resulted in

[497] U.S. Department of Commerce, "Intellectual Property and the U.S. Economy: Industries in Focus," March 2012.

[498] Office of the U.S. Trade Representative (USTR), "2012 Special 301 Report," April 2012, http://www.ustr.gov/sites/default/files/2012%20Special%20301%20Report_0.pdf; and Office of the USTR, "2013 Special 301 Report," May 2013, http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf.

[499] Office of the Secretary of Defense, Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013," prepared for Congress, Washington, D.C., 2013, 36, http://www.defense.gov/pubs/2013_China_Report_FINAL.pdf.

the compromise of at least three major defense contractors.[500] The same attack compromised security at an estimated 720 companies, including 20% of the Fortune 100.[501] Through another series of attacks, dubbed operation Shady RAT, it was discovered that petabytes of highly proprietary information, including sensitive military and infrastructure data, had been siphoned off from the U.S. Government and its allies, supranational organizations such as the United Nations, and many other sovereign nations and independent organizations over a period of more than five years.[502] Former General Keith Alexander, then the commander of the U.S. military's Cyber Command, said that one U.S. company alone lost $1 billion worth of intellectual property over the course of a couple of days.[503]

The onslaught of such attacks has been so significant that in May of 2014 a Federal grand jury indicted five Chinese military hackers, who for all intents and purposes appeared to be working to advance the ability of Chinese state-owned enterprises when they were negotiating with U.S. firms or unions. They are alleged to have stolen trade secrets and other sensitive business information, using cyber espionage for economic advantage.[504] The Chinese were after Westinghouse Electric, U.S. subsidiaries of SolarWorld AG, U.S. Steel, Allegheny Technologies and Alcoa. [505]

Smaller cases are most likely to reach indictments and prosecutions. In one case, international hackers were charged with breaking into computer networks of prominent technology companies and the U.S. Army and stealing more than $100 million in intellectual property and other proprietary data. The alleged cyber theft included software and data related to the Xbox One gaming console and Xbox Live online gaming system; popular games such as "Call of Duty: Modern Warfare 3" and "Gears of War 3"; and proprietary software used to train military helicopter pilots.[506]

The New York Times, the Wall Street Journal, and the Washington Post all disclosed that they believe their networks were compromised by intrusions that originated in China. A reasonable motive for targeting media is to identify reporters' sources for reporting that the Chinese government may not condone.

In another case, in August of 2014 a Federal grand jury indicted a Chinese national on five felony offenses stemming from a computer hacking scheme that involved the theft of trade secrets from American defense contractors, including The Boeing Company, which manufactures the C-17 military transport aircraft. The indictment alleges that the indicted Chinese national worked with two unindicted co-conspirators based in China to infiltrate computer systems and obtain confidential information about military programs, including the C-

[500] Zeljka Zorj, "RSA Admits SecurID Tokens Have Been Compromised," Help Net Security, June 7, 2011, http://www.net-security.org/secworld.php?id=11122.

[501] Brian Krebs, "Who Else Was Hit by the RSA Attackers?" Krebs on Security, web log, October 2011, http://krebsonsecurity.com/2011/10/who-else-was-hit-by-the-rsa-attackers.

[502] Peter Bright, "Operation Shady Rat: Five-Year Attack Hit 14 Countries," Ars Technica, August 3, 2011, http://arstechnica.com/security/news/2011/08/operation-shady-rat-five-year-hack-attack-hit-14-countries.ars; and "Massive Global Cyberattack Targeting U.S., U.N. Discovered; Experts Blame China," Fox News, August 3, 2011, available at http://www.foxnews.com/scitech/2011/08/03/massive-global-cyberattack-targeting-us-un-discovered-experts-blame-china.

[503] Ellen Nakashima, "In a World of Cybertheft, U.S. Names China, Russia as Main Culprits," *Washington Post*, November 3, 2011.

[504] http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[505] Pete Williams, U.S. Charges China with Cyber-Spying on American Firms, http://www.nbcnews.com/news/us-news/u-s-charges-china-cyber-spying-american-firms-n108706, accessed March 19, 2015

[506] http://www.justice.gov/opa/pr/four-members-international-computer-hacking-ring-indicted-stealing-gaming-technology-apache

17 transport aircraft, the F-22 fighter jet, and the F-35 fighter jet.[507] It is not yet known what the economic value of the loss of this intellectual property is, but it is clear that it provides a significant advantage to Chinese military aircraft producers.

The NextGov.com article on Federal agencies' capacity to bounce back from cyberattacks that wipe out data reported that those Federal agencies that protect intellectual property as part of their business invest to protect it. In a recent budget, the Department of Energy devoted $218 million; the Pentagon—$7 billion; NASA—$86 million; and the tiny National Science Foundation—$150 million for cybersecurity.[508]

It is reasonable to expect the frequency of such attacks to continue to increase between 2015 and 2020. It is likely that there will be an even greater increase in the following industries, based on their alignment with the Chinese 12th 5-Year Plan for National Strategic Emerging Industries:

- New energy auto industry
- Energy-efficient industry
- Advanced environmental protection industry
- Resource recycling industry
- Next generation information network industry
- Fundamental industry of core electronics
- High-end software and new information service industry
- Bio-pharmaceutical industry
- Bio-medical engineering industry
- Bio-breeding industry
- Bio-manufacturing industry
- Aviation equipment industry
- Satellite and its application industry
- Rail transportation equipment industry
- Marine engineering equipment industry
- Intelligent equipment-manufacturing industry
- Nuclear energy technology industry
- Wind energy industry
- Solar energy industry
- Biomass industry

[507] Edvard Pettersson, Chinese Man Charged in Plot to Steal U.S. Military Data http://www.bloomberg.com/news/articles/2014-07-11/chinese-citizen-charged-with-hacking-boeing-computer-in-u-s- accessed March 5, 2015

[508] Alia Sternstein, NextGov.com, Most Federal Agencies Wouldn't be able to Bounce Back From a Sony Hack http://www.nextgov.com/cybersecurity/2014/12/most-agencies-wouldnt-be-able-bounce-back-sony-hack/101658/ accessed March 5, 2015

- New functional material industry
- Advanced structural material industry
- High-performance composite material industry[509]

Cyber Extortion or Terrorism

Introduction

In recent years, we have seen attacks where the perpetrator was using their attack to influence others. This has been seen as a form of extortion by criminals, as a politically-motivated prank by terrorist groups, and as a threatening exercise of powers by nation-states displeased with the actions of companies in the U.S. While each of these manifestations has different direct effects, the indirect effect of a culture of supersized cyberbullying is a common result.

Scenario	Consequences	Vulnerabilities	Threats
Victim's data is destroyed, encrypted, or the victim is extorted with the threat of loss of access to their data	The theft and/or destruction of data leading to economic losses to recover from threat actors or to rebuild what was lost.	Inadequate malware or virus detection. Lack of logical security, monitoring activities, data back-up, and training of employees.	Criminal hackers are the most likely threat actors, and, in some cases, those with political motivations.

Table 25: Cyber Extortion or Terrorism Scenario Type 1

There are many alternate approaches to conducting an attack like this. Sometimes the result is significant and existential to the organization that was attacked. In other cases it is a small incident in the history of an organization. Unfortunately, the easiest way out is often to pay the ransom.

In a smaller impact attack, a virus called Cryptowall managed to bypass spam filters and firewalls and infected the police-department computer system in Durham, New Hampshire, when an officer opened an infected attachment on an email. By the next morning, they had widespread problems on the computer systems. This type of attack uses software that encrypts a user's hard drive, restricting them from accessing their own data. It holds it with a timer and a threat of destruction, until they pay a ransom. The town refused to pay the ransom, and the manager of the IT systems took the department's computer system offline, dealt with the problem, and reloaded their system with the backup files. [510] Their success in managing through this incident was largely attributable to the way they backed up their files.

Another more sophisticated and actively managed attack had a much more devastating impact on its victim. The code-hosting company Code Spaces was hit by a DDoS attack and then extorted

[509] Yao Lu, http://www.china-briefing.com/news/2012/07/25/china-releases-12th-five-year-plan-for-national-strategic-emerging-industries.html#sthash.dqWt0NAX.dpuf, accessed March 10, 2015

[510] Virus Infects Police Computer System In Durham NH, http://boston.cbslocal.com/2014/06/06/virus-infects-police-computer-system-in-durham-nh/ accessed March 20, 2015

by a hacker who had gained control of the firm's Amazon EC2 control panel, hoping to get paid in exchange for returning control of operations to Code Spaces. Code Spaces refused to comply, and quickly regained control of the account by changing password. The hacker recognized what was happening, used back-up logins that he had created, and started deleting files. Code Spaces revealed that "most of our data, backups, machine configurations and offsite backups were either partially or completely deleted." They were put out of business.[511]

The case of the Sony Pictures Entertainment hack where large amounts of intellectual property PII and other sensitive information was stolen was more complex. Recent evidence suggests that the intrusion that prepared for this attack began more than a year prior to its discovery in November 2014.[512] Director of National Intelligence James Clapper, speaking at conference at Fordham University, said the North Korean military's Reconnaissance General Bureau was responsible for "overseeing" the attack against Sony.[513] If this is true, it suggests that North Korea was watching for potentially offensive movies and began preparing to punish Sony well before they were ready to release the film.

In the case of the Sony attack, several exploits were used. The hackers extracted confidential data and then installed malware to erase data from the servers.[514] In the days following this hack, the perpetrators began leaking yet-unreleased films and started to release portions of the confidential data to attract the attention of social media sites, although they did not specify what they wanted in return.

Sony Pictures set aside $15 million to deal with ongoing damages from the hack.[515] While Sony made substantial additional investments in cybersecurity after this attack, according to Assistant Director Joseph M. Demarest, Jr., the head of the FBI's Cyber Division, an attack like this would have "slipped and gotten past 90 percent of the net defenses that are out there today in private industry."[516]

In such a data-destruction case, Government agencies would be in a particular trouble. As reported byNextGov.com, "a file-wiping attack such as the Sony Pictures Entertainment hack could bring major Federal departments to their knees, because most have no data-loss contingency plans, according to the latest figures on compliance with government cybersecurity laws. Further, unplugging systems to contain damage, as Sony did, would impair an agency's ability to carry out constitutional duties, some former Federal cyber-leaders say."[517] It is likely that targeted organizations will all have to learn how to operate in the trade-space between different types of risk.

[511] 6 Recent Real-Life Cyber Extortion Scams http://www.darkreading.com/attacks-breaches/6-recent-real-life-cyber-extortion-scams/d/d-id/1278774, accessed March 20, 2015

[512] Zetter, Kim (December 3, 2014). "Sony Got Hacked Hard: What We Know and Don't Know So Far". *Wired*. Accessed January 4, 2015

[513] FBI head details evidence that North Korea was behind Sony hack, http://touch.latimes.com/#section/-1/article/p2p-82479451/ accessed March 20, 2015

[514] Palilery, Jose (December 24, 2014). "What caused Sony hack: What we know now". CNN Money. Retrieved January 4, 2015.

[515] Frizell, Sam (February 4, 2015). "Sony Is Spending $15 Million to Deal With the Big Hack". *Time*. Retrieved February 4, 2015.

[516] House Homeland Security Chairman Michael McCaul, "Preventing a 'cyber Pearl Harbor': The Hollywood hack attack revealed the need to upgrade cybersecurity," *The Washington Times*, January 8, 2015, http://homeland.house.gov/news/mccaul-op-ed-preventing-cyber-pearl-harbor-washington-times.

[517] Alia Sternstein, NextGov.com, Most Federal Agencies Wouldn't be able to Bounce Back From a Sony Hack http://www.nextgov.com/cybersecurity/2014/12/most-agencies-wouldnt-be-able-bounce-back-sony-hack/101658/ accessed March 5, 2015

While the sophistication of these attacks varies and simpler individual attacks might be less consequential, in aggregate, a simple ransomware like Cryptolocker has affected at least 250,000 victims. Profits made from people complying with the demands can produce several million dollars per day.

The trend towards increasing complexity is likely to continue. The real consequences of these attacks vary by the organization, but as American work is commonly built on information and data, attacks that threaten to keep our data from us can be devastating. The ability of an organization to manage through such an attack and have a backup that cannot be affected by the same incident is critical to controlling its consequences.

Scenario	Consequences	Vulnerabilities	Threats
Victim's web-enabled communications are hijacked by the attacker, who uses it to convey their own message for political purposes, or just to embarrass authorities	The consequences of these attacks are costs borne by the victim for regaining control and dealing with the bad publicity.	Lack of security (physical and/or logical), monitoring activities, data back-up, and training of employees.	Criminal hackers are the most likely threat actors.

Table 26: Cyber Extortion or Terrorism Scenario Type 2

In January 2015, Twitter accounts for WBOC, a Salisbury, Maryland-based television station, and the Albuquerque News Journal in New Mexico were both hijacked by a hacker claiming to be sympathetic to terrorist group Islamic State of Iraq and the Levant, or ISIL. The hacker named "CyberCaliphate" used the Twitter accounts to post pictures and tweets throughout the day claiming to have classified information from Federal investigations into terrorist groups. The station's website was also hacked, with the top story being changed to one posted by "CyberCaliphate" before the station took it down. The station recovered control of its website on its own but had difficulty regaining control of its Twitter account.[518] A similar bout of attacks by ISIS sympathizers took place in March 2015 as well.

Other takes on this type of scenario have included taking over electronic highway messaging systems, modifying organizational intranets, and other efforts to pull pranks, embarrass or annoy the victims.

These types of attacks are not necessarily sophisticated but they are increasing in scope, with multiple organizations being attacked *en masse*. The consequences of these attacks are costs borne by the victim for regaining control and dealing with the bad publicity. However, the indirect consequences are not significant, except possibly to further the social divide between people who suspect others of being radical Islamists and those who are apt to be suspected.

In January 2015, Twitter accounts for WBOC, a Salisbury, Maryland-based television station, and the Albuquerque News Journal in New Mexico were both hijacked by a hacker claiming to be sympathetic to terrorist group Islamic State of Iraq and the Levant, or ISIL. The hacker named "CyberCaliphate" used the Twitter accounts to post pictures and tweets throughout the day

[518] Delmarva Now, WBOC Twitter, website hacked by ISIL supporters, http://www.delmarvanow.com/story/news/local/maryland/2015/01/06/wboc-twitter-hacked/21341645/ accessed March 21, 2015

claiming to have classified information from Federal investigations into terrorist groups. The station's website was also hacked, with the top story being changed to one posted by "CyberCaliphate" before the station took it down. The station recovered control of its website on its own but had difficulty regaining control of its Twitter account.[519] A similar bout of attacks by ISIS sympathizers took place in March 2015 as well.

Other takes on this type of scenario have included taking over electronic highway messaging systems, modifying organizational intranets, and other efforts to pull pranks, embarrass or annoy the victims.

These types of attacks are not necessarily sophisticated but they are increasing in scope, with multiple organizations being attacked *en masse*. The consequences of these attacks are costs borne by the victim for regaining control and dealing with the bad publicity. However, the indirect consequences are not significant, except possibly to further the social divide between people who suspect others of being radical Islamists and those who are apt to be suspected.

Scenario	Consequences	Vulnerabilities	Threats
Distributed Denial of Service Attack (DDoS) alone	The consequences of these attacks vary based on the goals of the attacker and range from data and economic loss to a loss of public confidence.	Lack of security (physical and/or logical), monitoring activities, or redundancy.	Given the varied reasons for a DDoS attack, the threat could come from any number of actors.

Table 27: Cyber Extortion or Terrorism Scenario Type 3

In the recent past, many offered the opinion that a DDoS was unsophisticated and likely to decline as a source of cybersecurity concerns. It is true that many of the very powerful DDoS attacks experienced in recent years have served as a smokescreen that distracted the cybersecurity staff while sophisticated break-ins and data extractions took place. However, DDoS alone remains a useful tool for adversaries who simply want to punish their victim. The exploit gives an adversary the ability to deny a victim of the normal commerce that would take place over their website or to embarrass them in the eyes of the general public. For many adversaries this is either sufficient, or at least good enough for the time being.

In 2014, DDoS attacks increased in size and power. Incapsula, a security company that specializes in protecting company websites, reports that such attacks more than tripled from December through February over the same period a year earlier. Incapsula labels DDoS "the weapon of choice" for hackers these days, in part because technology is making it increasingly convenient and powerful.[520] According to Verizon's most recent Data Breach Investigations Report, an attacker can rent a botnet for only $10 an hour. [521] But a botnet is just one element in a successful, large-scale DDoS attack. A popular method of increasing the size and power of DDoS attacks is to use a domain name system (DNS) amplification attack to take advantage of

[519] Delmarva Now, WBOC Twitter, website hacked by ISIL supporters, http://www.delmarvanow.com/story/news/local/maryland/2015/01/06/wboc-twitter-hacked/21341645/ accessed March 21, 2015

[520] Downloadable PDF, http://lp.incapsula.com/ddos-report-2014.html accessed March 5, 2015

[521] Downloadable PDF, http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf , accessed March 5, 2015

open recursive or authoritative servers to flood a target with DNS-responsive traffic. This works by amplifying the responses, at a rate of approximately 70:1. [522]An attacker can design his attack using a variety of contributing tools in an effort to exhaust the targets' resources.

Recent examples include the Sony DDoS Sony's PlayStation Network and Sony Entertainment Network in August 2014. An attack of this sort does not just cost the company the resources necessary to defend against the attack. When their customers try to access their sites and are frustrated, they often move on. Gaming service providers are very concerned about churn, with their regular customers' moving to competitors [523] Two different groups laid claim to the August Sony attacks, adding a tweeted bomb threat against an executive's flight in one of these claims.

Another retaliatory strike was experienced by the St. Louis County, Missouri police department, when their website and email servers were brought down in apparent protests over the shooting of Michael Brown. [524] A review of the Threat and Hazard Risk Identification and Assessment (THIRA) results provided to the Federal Emergency Management Agency reveals that state and local emergency planners look at incidents such as this as an indication of the potential use of this exploit as a way to complicate their responses in emergencies, such as the response to a natural disaster.

Other examples of DDoS attacks reported by Verizon include the 2012 and 2013 DDoS attacks on financial institutions claimed by the Izz ad-Din al-Qassam Cyber Fighters. This group appears to have been protesting an offensive film trailer hosted on YouTube. CNN reported, however, that it may be that the group was simply jumping on the attacks to promote their protest, noting that Sen. Joe Lieberman placed the blame on Iran. The goals of the threat actors may not be as relevant as the impact of the incidents on the targets. The resources of major financial institutions make them better equipped to fight against such onslaughts, but the cost of these attacks was still significant.

Attacks on Industrial Control Systems

Introduction

Industrial control systems (ICS) support the efficient and safe operation of large complex interconnected physical systems, such as those in major manufacturing plants, water purification and distribution systems, pipelines transporting petroleum products or natural gas, systems operating the electrical transmission and distribution grid, etc. For much of this infrastructure, ICS integration is decades old, incorporated with the primary purpose of increasing system reliability, and focused on infrastructure operating requirements. At that time, cybersecurity risks associated with this internet-based technology was not foreseen as a measurable business risk – assessed as low risk or not well understood. Owners and operators also range in their corporate risk tolerance, which can be based on a multitude of factors that vary across industrial sectors and across individual companies. Fast forward to the present day, we now find the concerns over cybersecurity risks are leading topics of discussion on corporate Board agendas.

[522] Anatomy of a DNS DDoS Amplification Attack. https://www.watchguard.com/infocenter/editorial/41649.asp, accessed April 27. 2015

[523] Charlie Osborne, Sony PlayStation Network struck by DDoS attack, bomb threat grounds executive http://www.zdnet.com/article/sony-playstation-network-struck-by-ddos-attack-bomb-threat-grounds-executive/

[524] Dara Kerr, Ferguson, Mo., police site hit with DDoS attack, http://www.cnet.com/news/st-louis-police-website-suffers-ddos-attack/ accessed March 5, 2015

It is noteworthy that the ICS-CERT FY 2014 Incident Response statistics showed that 55% of the incidents reported to them involved advanced persistent threats (APT) or sophisticated actors. Other actor types included hactivists, insider threats and criminals.[525] Attack types include attempts to exfiltrate ICS information. There are several key factors that influence the consequences associated with cyberattacks on ICS: the speed of the operations of the infrastructure under attack, the role of humans in the decision making processes for the operation of the infrastructure, and the number of opportunities to mitigate the direct effects of an attack before the full range of possible consequences materialize. Such adversaries are typically associated with a high degree of uncertainty and risk, as they often will expend a great deal of resources establishing themselves within a control system without a direct economic or short-term political motive.

Over the past few years, tools such as SHODAN, Google, and other search engines have enabled researchers, and really, the general public, to discover and identify a variety of ICS devices that were not intended to be Internet facing. Adding to the threat landscape is the continued scanning and cataloguing of devices known to be susceptible to emerging vulnerabilities. The increasing body of public knowledge about ICS, coupled with these tools, lowers the level of expertise necessary to successfully locate Internet-facing control system. Many of these devices have not been configured with adequate authentication mechanisms, making it easy to directly access the systems by both opportunists and sophisticated threat actors. As tools and adversary capabilities advance, we expect that exposed systems will be more effectively discovered and targeted by adversaries. Clearly, it has become more important for asset owners and operators to audit their network configurations and properly install their ICS devices behind patched VPNs or firewalls, and yet surprisingly few do, until they discover a problem and seek help.

Owners and operators vary in the clarity with which they focus on this problem. Some systems have been hacked, but with no apparent outcome, suggesting this is not a real problem. Some owners and operators respond to this discovery with little concern, because nothing happened. Others respond defensively and take action, concerned about the reality of sophisticated threat actors possibly having an ability to sabotage their systems in ways they have not yet imagined. The ODNI reports that:

> Russia’s Ministry of Defense is establishing its own cyber command, which—according to senior Russian military officials—will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia’s armed forces are also establishing a specialized branch for computer network operations[526].

The Worldwide Threat Assessment goes on to refer to private sector “computer security studies which assert that unspecified Russian cyber actors are developing means to access industrial control systems remotely. These systems manage critical infrastructures such as electric power grids, urban mass-transit systems, air-traffic control, and oil and gas distribution networks. These unspecified Russian actors have successfully compromised the product supply chains of three

[525] ICS-CERT Monitor September 2014-February 2015

[526] Clapper, James, Worldwide Threat Assessment

ICS vendors so that customers download exploitative malware directly from the vendors' websites along with routine software updates."[527]

If this undiscovered presence in their control system was used maliciously, the outcomes would vary tremendously based on the system, infrastructure subsector, the conditions surrounding the actual manipulation of the control system and more. Sometimes the adverse outcomes for the equipment and materials may be risks that may prove costly, but have low potential for life and safety impacts. Some sectors have such tight operating margins, that any costly errors are unacceptable. Other sectors have the margins available to exchange profits for safety and do so without concern that they could not make up the losses. Thus, owners and operators can range between highly risk-averse to accepting some forms of loss as a trade for avoiding others.

ICS-CERT conducts risk mitigation activities and incident response for critical infrastructure owners and operators. In FY 2014 Incident Response statistics reported that 55 percent of the incidents reported to them involved advanced persistent threats or sophisticated threat actors. Other actor types included hactivists, insider threats, and criminals.[528][529] When an organization is attacked by a sophisticated threat actor the organization is left with a high degree of uncertainty and incalculable risk. It is unclear to the victims what the adversary's motivations were. They doubt the explanations of computer security consultants and the Government. They wonder why these adversaries expend such a great amount of resources establishing themselves within this control system, without a direct economic or short-term political motive. Many find this type of uncertainty immobilizing. It is easier to deal with known problems than to try support decisions about such uncertain risks.

Illustrative of Government efforts to help clarify these risks, ICS-CERT and the FBI teamed up in 2014 to respond to sophisticated cyber-exploitation campaigns against U.S. infrastructure ICS. These campaigns involved different sets of malware, both of which used tactics to target and gain access to control systems environments. One of them, BlackEnergy, has been discovered within the controls that operate many infrastructure sectors. The BlackEnergy hacking campaign had been ongoing since 2011, but there is no evidence of any attempt to activate the malware to damage, modify, or otherwise disrupt affected systems. Havex, the other malware, also called Dragon Fly, has also been found in ICS. According to Joel Langill, security consultant and author of the *SCADAhacker* blog, "A lot of malware impacts control systems, like Conficker or Slammer," referring to two computer worms that caused headaches for tens of thousands of people using Microsoft. "Those have consequences on industrial environments, but ... Stuxnet, Dragonfly and now Black Energy have specific ICS payload components; they are targeting specifically industrial control systems. This is very disturbing."[530]

The Energy Sector led all others again in 2014 with the most reported incidents. ICS-CERT's continuing partnership with the Energy Sector provides many opportunities to share information and collaborate on incident response efforts. Also noteworthy in 2014 were the incidents reported by the Critical Manufacturing Sector, some of which were from control systems

[527] Clapper, James, Worldwide Threat Assessment

[528] ICS-CERT Monitor September 2014-February 2015

[529] An insider threat is one or more individuals with access or insider knowledge of an enterprise that allows them to exploit vulnerabilities, resulting in harm to the enterprise

[530] SECURITY: Secret meetings tackle back-to-back energy-sector cyberthreats, http://www.eenews.net/stories/1060008193, accessed March 24, 2015

equipment manufacturers. The ICS vendor community may be a target for sophisticated threat actors for a variety of reasons, including economic espionage and reconnaissance.[531]

The scenarios considered in this scoping assessment reflect a sample from the Energy Sector, based on the predominance of voluntarily reported incidents of this type to ICS-CERT. Owners and operators in the Energy Sector have noted the measurable value they receive in return for their partnership with ICS-CERT. In addition there is a scenario for the Water and Wastewater Sector. While water-system attacks are less commonly reported, state and local authorities have a high level of concern with them as is evidenced by their contributions to THIRA. There is no evidence that these types of attacks have been completed; which is to say, the results of ICS-CERT investigations into incidents of these types typically conclude that detection and mitigation mechanisms effectively employed prevented adversaries from fully executing intended attacks. The analysis below provides insights into the how the management of the targeted infrastructure may or may not provide a limiting effect on attacks of this type. It is likely that whatever alternate management controls owners and operators may have on the operation of their infrastructure would be severely stressed if there were coordinated complex attacks, as these alternate controls all rely more heavily on human operators.

In clarifying the potential impacts of cyberattacks on ICS, we have used a simple logic model and validated conclusions with representatives of the owner and operator community. This logic model focuses on identifying a series of related, but normally obscure conditions and effects, including:

- The role of information and communications technology in managing or monitoring the infrastructure’s equipment;
- The direct effects of lost confidentiality (data breaches), integrity (altered data or co-opted control), and availability (destroyed data or denial of service) on the various infrastructure systems;
- The availability and limitations of alternatives, such as human operators or back up mechanical devices, to perform the functions that the ICS normally controls;
- The potential infrastructure functional impacts that may result;
- The availability and limitations of infrastructure management alternatives that may address the infrastructure functional impacts.

[531] ICS-CERT Monitor, September 2014-February 2015

Scenario	Consequences	Vulnerabilities	Threats
Distributed campaign of attacks on natural gas pipeline system industrial control systems (ICS), timed to maximize the impacts on energy assurance	While an individual attack on a pipeline system can be adequately managed, a distributed attack could lead to shortages and customer outages. This would create a loss of revenue for the utility company and could adversely affect consumers.	Distributed nature of pipeline control systems. Integrated nature of systems allowing less secure devices that are directly connected to the Internet to be breached, thereby granting access to the more secure ICS.	Criminal hactivists, terrorist organizations, and nation states are the most likely threat actors.

Table 28: ICS Scenario Type 1

Natural gas transmission systems are those that deliver natural gas from the processers to local distribution companies, also known as the utility. They may be likened to a system that keeps the warehouses stocked. Because they ship large volumes that get split to different distribution networks, the pipelines have a large capacity. They are typically located away from populated areas and require compressors every 50–100 miles to keep the gas moving at the required rate. If a few of the compressors are damaged or not functioning as required, the movement of the gas may slow or stop. Transmission pipeline operators stop the movement of gas if there has been an accident with the pipeline in order to make the repairs. Typically, customers are unaffected by these shutdowns because of the resiliency of the pipeline systems to work around an incident area and to deliver product through back-up alternatives. Similarly, cyber-disruptions impacting the movement of gas through a pipeline may reduce the amount of gas that can be delivered. However, this can be mitigated in the short-term by stored reserves or alternative gas delivery paths.[532]

Local distribution systems have many localized branches, with reduced pressure and capacity as the system gets closer to the customer. The features of the distribution system make it very unlikely that a single disruption in a pipeline would affect all of their customers. Most service disruptions would more than likely impact smaller customer sets, if at all, which may be isolated for response and recovery.

Since the management of natural gas demands a strong safety culture, the industry is well versed in emergency controls that can be applied across many situations. These mandated controls may be used to mitigate the direct physical effects of cybersecurity incidents as well. There are also natural limits on what might happen on a single pipeline. For example, if a pipeline ruptures, a single release could lower system pressure, thus reducing the potential for further physical damage. In most cases, if control systems are found to be corrupted, pipelines can also be operated manually without these digital controls, though at a diminished rate.

Some areas of the country are much more dependent on natural gas. The demand for natural gas for heating and power generation during a harsh winter may be sufficient to cause shortages when combined with an unexpected incident. When a shortage occurs, it is sometimes possible to move gas from areas with more stored capacity to areas with a shortfall by diverting flow from other pipelines. Similarly, major natural gas users usually have contractual agreements to switch

[532] Office of Cyber and Infrastructure Analysis, Natural Gas Cyberdependencies, February 3, 2015

from natural gas to another fuel supply in the event of shortage, and smaller customers can reduce their use through conservation. Natural gas utilities place a very high priority on avoiding any service disruptions and use all of the options available to them to keep customers supplied and prevent natural gas appliance lights from extinguishing.

Pipeline operators recognize that despite the robustness of the pipeline system and the standard practices for managing many types of emergencies, the impacts of a broad-scale attack on their systems must be taken seriously. Operators were confronted with this challenge when an active series of cyber-intrusions targeting natural gas pipeline sector companies occurred in 2011–2012. This single campaign from an unknown source was identified by ICS-CERT through the proactivity of owners and operators' reporting and effective information sharing. The campaign, which started in December 2011 with sophisticated, targeted spearfishing and continued for months, extracted data that could facilitate remote unauthorized operations.[533]

Since ICS are in place to facilitate reliable and efficient operation of pipeline systems that span long distances, they have the effect of reducing the number of operators needed onsite at compressor stations to control compressors. As a result the standard risk management techniques associated with onsite personnel and effective for individual events may become much more challenging given a coordinated and distributed cyberattack. Responding to such an attack would be much more stressful for the industry, testing the usefulness of mutual aid agreements within the industry if owners and operators perceive themselves simultaneously under the same attacks. There are limits to mechanisms that bring in reserve workforce and emergency responders with equipment. Response may be based on the availability of these assets. Some emergency response planners have noted that the challenges of dealing with declining budgets have resulted in decisions to reduce back-up resources and increasingly depend on mutual-aid agreements. These agreements have limitations, especially when considering the possibility of large-scale attacks that may affect multiple jurisdictions.[534]

Repeated and persistent efforts are being made to create an undetected presence of malware within natural gas pipeline systems. The scale and sophistication of these attacks appear to be increasing. The consequences of such attacks, if they were to result in active exploitation of the ICS and affected the operation of the pipelines, would be very challenging to the owners and operators. Most of these impacts are felt within the natural gas industry. It would be unlikely that such an attack would result in outages that affected the customers, unless the scale of attacks was so great that it overwhelmed the combined capabilities of the human operators. If there were a significant regional gas outage, especially if it were timed to maximize the negative impact on the population, the normal procedures would be to provide warming centers for those who are affected and then systematically manage the problem. Boulder County, Colorado experienced this problem in December 2103, when temperatures were in the single digits. Their experience, which affected 7,200 customers, provides a useful example.

The Red Cross opened warming centers to help those who could not manage the temperature drop in their homes. The utility called in extra resources from elsewhere in Colorado, and from

[533] ICS-CERT Monthly Monitor, June/July, Gas Pipeline Cyber Intrusion Campaign-Update; http://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jun-Jul2012.pdf.

[534] Deborah Strasheim, Mutual Aid a concern for region's fire departments, http://www.theday.com/article/20140628/NWS01/306289976 , accessed March 6, 2015

four other states. The crews visited all customers and, turned off affected gas lines so the pressure in the lines could be restored. They were told they could not relight appliances themselves, as they would risk damaging the appliances or equipment, as well as placing themselves and their families in danger.

In summary, cyberattacks on natural gas pipeline systems continue. Data from ICS-CERT demonstrate the scale and scope of these attacks are increasing, though none of these have resulted in sabotage of the system. Nevertheless, the types of exploits observed reflect an evolving capacity to do so. The consequences of attacks that have physical effects are not likely to be devastating or have long-term impacts on customers. Natural gas pipeline systems must comply with the U.S. Department of Transportation pipeline safety regulations which are intended to prevent or minimize natural gas pipeline incidents. Owners and operators, government authorities and not-for-profits have demonstrated the capacity to manage gas delivery and reliability even during stressful periods. Attacks that combine cyber and physical tactics are much more likely to cause significant damage. Such attacks require more resources from perpetrators to understand pipeline operations, to assess pipeline infrastructure vulnerabilities and to gain access to the ICS.

Scenario	Consequences	Vulnerabilities	Threats
Cyberattack on ICS in a drinking-water system results in contaminated water	The consequences of an attack on the water system would be minimal to the public given the amount of manual and system checks currently in place. However, any type of communicated risk can have an adverse effect on public confidence in the quality of the product and the organization providing it. The greatest impact would be to the water utility in an increased need for additional cybersecurity technology.	Distributed nature of pipeline control systems. Lack of monitoring or systems, logons, and third party vendors. Integrated nature of systems allowing less secure devices that are directly connected to the Internet to be breached, thereby granting access to the more secure ICS.	Criminal hactivists, terrorist organizations, and nation states are the most likely threat actors.

Table 29: ICS Scenario Type 2

Drinking-water systems often use ICS for storage, treatment, and distribution systems. These ICS are involved in monitoring the operations of the equipment, monitoring the quality of water, and controlling different functions to execute the operations of the system. Many water utilities have ICS that are isolated from general IT enterprise systems, but trends of increasing connectivity and automation are increasing cybersecurity risks. Water utility IT services may be remotely operated by external entities which could result in unsecure remote access leaving utilities unable to detect or prevent unauthorized access.[535] Furthermore, it is not uncommon for utilities to maintain their electronic records solely for the purpose of operating safely and efficiently. They do not always consider the forensic value of recording logon events, assuring

[535] Office of Cyber and Infrastructure Analysis, Critical Infrastructure Security and Resilience Note: Water and Wastewater Systems Sector Cyberdependencies, August 22, 2014

individual usernames, or maintaining network monitoring systems and operating system records for later use.[536]

A cyberattack may cause a brief interruption or degradation within the drinking water and wastewater services. However, water infrastructure can be operated manually in the event of an incident, preventing prolonged inoperability. There is little risk of regional or national impact to public health and the economy from a single cyberattack against a water or wastewater system. A cyberattack that compromises control systems in a drinking water system is unlikely to have an immediate effect on customers, due to the existing water supply within the system.[537]

The effect of overtreatment is not toxic. The water will have chemical odors and taste, but it is not harmful to the public. The effect of under-treatment could result in pathogens being found in the water, but this still does not mean that the public will be impacted. The time delays between a gallon of water undergoing treatment and when it actually comes out of a faucet can be measured in hours or even days. This gives operators a chance to correct undertreated water while it is still in the transmission and distribution system. Even if all of the backstops fail, and undertreated water reaches the faucet, the outcome is comparable to other incidents, such as water-main breaks, electrical outages, which may force boil-water notices, or some other advisory not to use the water until the conditions have been cleared.

Risk perception is often a matter of perspective. National authorities may view boil-water or Do-Not-Use notices as a routine and appropriate action for water system operators who have operational problems. Many of the owner-operators, however, experience these problems infrequently and are more risk averse. Furthermore, they believe that the public would respond differently if the same notice went out because of a cyberattack.

Managing these risks are problematic as well. Sometimes they do not have as much control over their own IT systems as other infrastructure operators. The IT or cybersecurity staff at a water system may be limited in their authority. They are often part of a larger municipal enterprise with shared IT systems. This creates a layer of bureaucracy that may make it harder to execute needed changes within the enterprise architecture. The costs of cybersecurity are significant for a water utility. They do not have the authority to simply charge more for water to cover these expenses. Any rate hikes must be approved by an oversight authority, such as a planning commission. Finally, water systems often contract with third parties to manage and update their control systems. This model of operations may seem less costly, but it typically results in their devices being exposed to the Internet, leaving them uncertain about who is accessing these systems.

There have been instances where cyberattacks have had physical consequences in the Water and Wastewater Systems Sector. In one instance, the system that controlled a vital operating function was hacked by a foreign national, who used it as his own distribution system for email or pirated software. The unauthorized traffic used so much of the system's capacity that operations were impacted, but the facility was able to manage and the water quality was not impacted.[538] In a more removed example, in 2000, at a sewage treatment plant in Queensland, Australia, a former employee of a software company hacked into the SCADA system releasing over 264,000 gallons

[536] ICS-CERT Monitor, Water Treatment Facility Control System Anomalies, May-August 2014

[537] CISR Note: Water and Wastewater Systems Sector Cyberdependencies

[538] Jerome, Sara. *Water Sector Eyes Federal Cybersecurity Efforts*. Water Online. July 31, 2013, http://www.wateronline.com/doc/water-sector-eyes-federal-cybersecurity-efforts-0001, accessed March 6, 2015

of raw sewage into the surrounding environment. The situation in Queensland is a noteworthy example as this vulnerability may be found in U.S. water and wastewater systems that have not taken extra measures to prevent it.

Also, cyberattacks could potentially result in breakage of pipes, treatment equipment, pumps, etc. If an attack were to result in breakage, the consequences would go up. Some state and local planners want to prepare for scenarios with distributed and coordinated cyber-attacks on ICS that result in water treatment failures and broken infrastructure. Such attacks have not been reported, but may be feasible. The concerns about water contamination are noted above. Broken infrastructure would add significantly to costs, and increase the stress on a sector with very tight operating margins. Concerted public and private collaboration has considered the possibility of such physically destructive attacks. The safety-engineering designs seem likely to intervene to protect pumps and valves. There is a low level of confidence that significant physical destruction is even feasible through attacks on the water infrastructure.

The costs of replacing broken equipment within a drinking water system will vary. As a rough planning guide, equipment that is concealed below the surface, delaying the recognition of the problem and requiring excavation to address it, will be more costly and disruptive to replace than comparable equipment closer to the plant. The costs and disruption increase significantly if this is in a highly trafficked area. This considers just the costs to the utility. If water service was lost in an area, the local and regional economic losses would be far greater. If there were a widespread outage, the time to repair and replace the damaged infrastructure could be significant.

It is important to maintain flow in water distribution systems. If pipes become empty, the external pressure on the pipes is not balanced by an interior pressure. This may result in seepage into the pipes and contamination of the water, which would be mitigated by a boil water notice. Some consider it is also feasible there might be fractures in older or more fragile pipes, and repairs, replacements and environmental impacts can be very costly.[539]

There have been no observed incidents of drinking water equipment breakage. Comparable equipment has been attacked with relatively minor consequences. In 2007, in Willows, California, a failure of physical security allowed a former employee to gain access to a SCADA system and install unauthorized software which damaged the SCADA system itself, but not the irrigation system it was managing.[540]Another example of the potential harm that may stem from an information security problem was the 2005 failure of the Taum Sauk Dam in Missouri. This dam did not contain a drinking water reservoir, but rather a reservoir built on top of a mountain to facilitate hydro-generation. It was an earthen embankment dam that operated by releasing water during peak electrical demand hours, and then pumping the water back up during off-peak hours. There was a difference between the data reported by gauges at the dam and gauges at a remote monitoring system which led to water continuing to be pumped, even though the reservoir was already at maximum capacity. The resulting overflow led to a catastrophic

[539] Office of Cyber and Infrastructure Analysis, Critical Infrastructure Security and Resilience Note: Water and Wastewater Systems Sector Cyberdependencies, August 22, 2014

[540] U.S. Government Accountability Office, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, GAO-08-119T, October 17, 2007. Page 7.

release.[541] It may be rare for drinking water reservoirs to be situated this way, or for the status of drinking water reservoir to be monitored less closely. While this type of loss seems a plausible example of significant physical damage that could occur, Environmental Protection Agency (EPA) subject matter experts maintain that the peculiarities of the hydroelectric reservoir involve conditions that cannot be found in water systems.

Individual cybersecurity incidents in the Water and Wastewater Systems Sector typically do not have offsite consequences, but when they do, the consequences are unlikely to be greater than those that arise occasionally from other causes, such as equipment malfunctions or flooding. All infrastructure sectors depend on drinking water and wastewater systems to some degree, and would not be able to function for extended periods of time without these systems. Any suggestion that there are likely to be cascading infrastructure consequences from individual cybersecurity incidents at water or wastewater infrastructure would be misleading and overstated, because a cybersecurity incident is unlikely to result in a significant denial of water or wastewater services. The potential for a temporary loss of water or wastewater services to have a cascading effect in another sector is small and localized, but could be significantly greater if coordinated distributed attacks impacted many parts of an individual large system, or affected many systems.

Cyberattacks on water and wastewater systems continue, with sophisticated actors often the perpetrators. It is not clear if the scale and scope of these attacks is increasing; if so, they are not increasing significantly. The consequences of isolated attacks that are actually able to contaminate the water system through under-or over-treatment are not likely to have a devastating effect. Water moves slowly enough through a system that there are opportunities to discover, through additional monitoring, that the water quality is incorrect and to intervene and flush the water before it is released. Attacks that result in physical damage or those that combine cyber- and physical tactics are much more likely to cause significant damage and costly consequences. Water system information security incidents continue to increase in frequency, though very few to date have had actual physical consequences. These, however, are not the type of scenarios where sophisticated actors have invested in developing the presence and capacity to sabotage the system. It is unclear if these exploits are actually increasing, or if it is just due to owners and operators revealing them at a greater rate. In either case, the sophisticated and coordinated attacks that result in devastating outcomes have not occurred.

[541] National Weather Service Weather Forecast Office, December 14, 2005 Taum Sauk Dam Failure at Johnson's Shut-In Park in Southeast Missouri. http://www.crh.noaa.gov/lsx/?n=12_14_2005.

Scenario	Consequences	Vulnerabilities	Threats
Complex coordinated attack on the grid is conducted so as to maximize physical damage and power outage	The most serious consequences of a successful cyberattack on the grid would be associated with attacks that succeeded in destabilizing the grid by removing a large proportion of either generation or load resulting in rolling blackouts.	Distributed nature of electricity substations. Lack of monitoring or systems, logons, and third party vendors. Integrated nature of systems allowing less secure devices that are directly connected to the Internet to be breached, thereby granting access to the more secure ICS.	Criminal hactivists, terrorist organizations, and nation states are the most likely threat actors.

Table 30: ICS Scenario Type 3

In November 2014, Admiral Michael Rogers, the Director of the National Security Agency and Commander of the U.S. Cyber Command testified before the House (Select) Intelligence Committee that sophisticated attacks from nation-states had the potential to “shut down the entire U.S. power grid.”[542] Concern about cyberattacks on the electrical grid is reflected in a large number of the scenarios identified from a review of THIRAs.

Electric power networks are required to be resilient to the loss of any single component (including generation units, high-voltage transmission lines, and transformers) under the reliability standards developed and enforced by the North American Electric Reliability Corporation (NERC), which oversees eight regional reliability entities and encompasses all of the interconnected power systems of the contiguous United States, Canada and a portion of Baja California in Mexico. Each of these regional entities is also required to maintain an “operating reserve margin” of available generation capacity that can be called up within minutes to mitigate the loss of generation sources due to an unplanned outage.

The most serious consequences of a successful cyberattack on the grid would be associated with attacks that succeeded in destabilizing the grid by removing a large proportion of either generation or load. A cyberattack could theoretically be designed to disrupt power generation directly through its control system or by causing a precipitous drop in demand. This drop in demand could be achieved by disconnecting portions of the transmission network, which could cause generation plants to trip offline to avoid damaging the turbines. The consequences of an attack will depend on two factors: the amount of generation capacity taken out of service and whether the equipment is physically damaged. If a sufficient amount of generation is taken offline, low voltage and outage conditions could result. If equipment is physically damaged, restoration will take far longer than if it has only been disconnected. Even if equipment is not damaged, operators would still need time to investigate the causes, assess operability, and restart generators.

[542] National Security Agency Hearing of the House (Select) Intelligence Committee; Subject: "Cybersecurity Threats: The Way Forward," transcript at www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf, accessed March 5, 2015.

Transmission networks combine cyber-dependent control systems and the potential for high consequences from outage. The high-voltage transformers used in electric power transmission, in particular, would be expensive and difficult to replace if damaged. However, it is not clear that a cyberattack would be able to physically damage multiple transformers, because this equipment is protected by multiple protection layers, including some protection layers built into the transformers, specifically designed to minimize the damage to transformers.[543] Replacing damaged extra-high voltage transformers would be expensive and logistically difficult as replacements can take up to 18 months to manufacture.

If enough generation is lost that the operating reserve margin is exhausted, the regional operators could call for utilities to shed load through voluntary conservation, exercising interruptible contracts, or implementing rolling blackouts as needed. Rolling blackouts are likely to be the worst-case consequence for the disruption of a small number of generation plants.

An attack on transmission network or generation equipment that disrupts a large number of assets on the network could have high consequences, perhaps similar to the 2003 Northeast Blackout, which affected an estimated 10 million people in Ontario and 45 million people in eight states in the U.S.[544] This would likely require a very well-planned and sophisticated attack, because even though multiple systems may use the same control system protocols, the protocols can be implemented differently; each time a system operator sets up the control system, there should be a unique set of access controls (e.g., passwords). Disconnecting or damaging a sufficiently large amount of generation could cause widespread blackouts and “islanding” of portions of the grid still operating. In addition to the time needed for assessment, operators would need to restore power gradually to maintain the stability of the grid as more generation returned to service. In the event of a complete regional blackout, certain generation stations capable of starting up without using offsite power would be the first to be restored, so that they could provide the offsite power needed to bring other sites back online.

Although the system is resilient to unplanned outages of one or two assets, such as may occur in the normal course of operation, it is not designed to cope with an intentional attack on many assets. Outages of this length obviously pose health and safety concerns, would incur business disruption costs, and stress the backup power provisions for critical infrastructure. There is also the potential for added psychological impact associated with the fact that the outage was caused by a cyberattack. This will likely shake the public’s confidence in critical infrastructure security and perhaps infrastructure regulators.

Modeling and simulation of electric power is well-developed and is used for the daily operation of electric power networks, planning for future network conditions, predicting the impacts of

[543] See for example GE Digital Energy, “Transformer Protection Principles,” www.gedigitalenergy.com/smartgrid/Mar07/article5.pdf , accessed March 9, 2015.

[544] Although advances in reliability standards make such an event unlikely today, this is an example of a cascade set off by a software bug in a control room alarm system. At the peak of summer demands for electric power, a transmission line sagged into an unpruned tree. This cascaded into an outage that affected an estimated 10 million people in Ontario and 45 million people in eight states in the U.S. because control room operators did not receive the alarm and respond in time. The fluctuating power on the network caused more than 508 generating units at 265 power plants to trip offline. Secondary impacts were felt to communications (including 911 services), water infrastructure, and electric rail transportation. See U.S.-Canada Power System Outage Task Force, “Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations,” April, 2004, at http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf, accessed March 3, 2015.

impending or hypothetical hazards, and optimizing network restoration. In addition to utilities and their authorities, numerous National Laboratories, universities, Government entities and others use commercially-available models, sometimes tailored to answer particular questions.[545] Thus, there is a wealth of information (historical data and modeling results) about how the electric grid might behave under various contingencies. Nonetheless, it is impossible to predict the outcome of any scenario with complete certainty. This is partly because the instantaneous conditions on the network can affect the outcome, and partly because it is impossible to know all the factors that will influence the decisions made by the people actually managing the grid.

Similarly, there is a wealth of information about cybersecurity and a strong motivation to protect the information and communications networks on which the electric grid increasingly relies. What is missing is a good understanding of how vulnerabilities in cyber infrastructure might play out in an attack scenario. This is likely to be a very thorny problem, as the answers will vary from region to region and perhaps, utility to utility, depending on the exact configuration of existing physical and virtual infrastructure.

For example, it is not clear to what degree a cyberattack could physically damage infrastructure. If damage is minimal, the impacts could be orders of magnitude less than the worst-case scenarios involving damaged high-voltage transformers. Even as widespread, disruptive, and costly as the 2003 Northeast Blackout was, most customers had power restored within 2 days. In contrast, although Superstorm Sandy affected a smaller number of customers, restoration required repairing or replacing a huge amount of equipment damaged by winds and flooding, and took much longer to complete. Still, the rate of restoration after Sandy was similar to that required for other strong, damaging storms; it took about 10 to 14 days to restore power to 95% of customers.[546] Clearly, the degree of physical damage to the system will be a key driver in the duration of an outage and therefore the human, economic, and social impacts.

For this reason, scenarios that combine cyber and physical attacks are likely to have the greatest potential consequences. For example, a cyberattack could make a physical attack more difficult to detect and mitigate, while physical damage could delay restoration and thereby magnify the impacts of a cyberattack. Combined attacks may be cyber-enabled physical attacks (in which cyber means are used to get access to enable a physical attack) or a physical-enabled cyberattack (in which physical means are used to access a control system, thereby allowing the system to be maliciously altered). Either type could have serious consequences.

Cyberattacks on the grid continue, with sophisticated actors often the perpetrators. The scale and scope of these attacks may be increasing, but if so, not significantly. The consequences of attacks that are only able to impact individual generators, or which do not cause significant physical damage are unlikely to have a devastating effect. Attacks that combine cyber- and physical tactics are much more likely to cause significant damage and costly consequences, and it is unclear if such attacks are being planned. Electric grid cybersecurity incidents continue to increase in frequency, including attacks by sophisticated actors appearing to establish the

[545] One example is the electric power analysis performed by DHS for hypothetical disaster scenarios or in response to real-world events. DHS is supported by the National Infrastructure Simulation and Analysis Center, a joint endeavor of Los Alamos and Sandia National Laboratories. For more information, see www.dhs.gov/office-cyber-infrastructure-analysis.

[546] Fahey, Jonathan, Associated Press, "Power Outages After Hurricane Sandy Weren't Unusually Long After All," November 16, 2012, at www.dailyfinance.com/2012/11/16/power-outages-after-hurricane-sandy-werent-unusually-long-after/, accessed March 3, 2015.

capability to sabotage the grid. The actual acts of sabotage are not attempted, however, and it is unclear if the risk of coordinated and effective sabotage of the grid through cyberattacks will happen.

Cyber 9/11

Introduction

There are quite a number of sources that have postulated that massive distributed attacks against infrastructure are expected, which would have massive debilitating effects on the U.S.. Starting back in 1991, when Winn Schwartau, then Director of the International Partnership against Computer Terrorism, warned against an electronic Pearl Harbor in his testimony before the House Subcommittee on Technology and Competitiveness of the Committee on Science, Space and Technology of the U.S. House of Representatives.[547] Members of the 9/11 Commission called attention to the threat in "Reflections on the Tenth Anniversary of the 9/11 Commission Report.[548] Homeland Security Secretary Janet Napolitano warned in January 2013 speech at the Wilson Center that a "cyber 9/11" could happen imminently. If it were to occur, it could cripple the country, taking down the power grid, water infrastructure, transportation networks and financial networks."[549]

The most recent assessment of the U.S. Intelligence community reduces the expectation for such a scenario. In his February 26, 2015 testimony before the Senate Armed Services Committee James Clapper, Director of National Intelligence stated that, "Rather than a 'cyber-Armageddon' scenario that debilitates the entire U.S. infrastructure, we envision something different," …"We foresee an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on U.S. economic competitiveness and national security."

Coincidentally, this speech followed a day after New York financial regulator Ben Lawsky predicted that a cyber-Armageddon would occur within the Financial Services Sector in the next decade. This reflects the importance of the viewpoint of those who are interpreting what is going on.

Scenario
Complex coordinated attack on significant infrastructure resulting in catastrophic outcomes

Cyber 9/11 Scenario Type 1 (description only)

The Internet and American Life project conducted by the Pew research firm on the subject released its findings in Digital Life magazine in 2015.[550] Their survey of 1,642 experts in the field found that 61 percent believe that by 2025, there will a major cyberattack that has caused widespread harm to a Nation's security and capacity to defend itself and its people. (By

[547] The record of the proceedings http://babel.hathitrust.org/cgi/pt?id=pst.000018472172;view=1up;seq=14#view=1up;seq=1 , accessed March 6, 2015

[548] Adam Goldman, 9/11 commission members warn of cyber attack threats, http://www.washingtonpost.com/world/national-security/911-commission-report-authors-warn-nation-of-cyberattack-threats/2014/07/21/82d0fb84-10e5-11e4-98ee-daea85133bc9_story.html accessed March 6, 2015

[549] Reuters, U.S. homeland chief: cyber 9/11 could happen "imminently", http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124?feedType=RSS&feedName=technologyNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+reuters%2FtechnologyNews+%28Reuters+Technology+News%29 accessed March 6, 2015

[550] http://www.pewinternet.org/2014/10/29/cyber-attacks-likely-to-increase/

"widespread harm," they specified significant loss of life or property losses/damage/theft at the levels of tens of billions of dollars.) Survey respondents provided the basis for their judgment, which the Pew researchers organized into four themes:

- Internet-connected systems are inviting targets. The Internet is a critical infrastructure for national defense activities, energy resources, banking/finance, transportation, and essential daily-life pursuits for billions of people. The tools already exist to mount cyberattacks now and they will improve in coming years—but countermeasures will improve, too.
- Security is generally not the first concern in the design of Internet applications. It seems as if the world will only wake up to these vulnerabilities after catastrophe occurs
- Major cyberattacks have already happened, for instance the Stuxnet worm and attacks in nations where mass opposition to a regime has taken to the streets. Similar or worse attacks are a given.
- Cyberattacks are a looming challenge for businesses and individuals. Certain sectors, such as finance and power systems, are the most vulnerable. There are noteworthy divides between the prepared and the unprepared.

The other 39 percent of the respondents believed that there would not be such a major attack by the year 2025. The justifications for their responses were grouped into the following lines of thought:

- There is steady progress in security fixes. Despite the Internet's vulnerabilities, a distributed network structure will help thwart the worst attacks. Security standards will be upgraded. The good guys will still be winning the cybersecurity arms race by 2025.
- Deterrence works, the threat of retaliation will keep bad actors in check, and some bad actors are satisfied with making only small dents in the system so they can keep mining a preferred vulnerability and not have it closed off.
- Hype over cyber-attacks is an exaggeration of real dangers fostered by the individuals and organizations that will gain the most from creating an atmosphere of fear.

Perhaps the most interesting outcome of this research is insight into how individuals who seem to be experts in a field, maintain inconsistent knowledge of current events in their area of expertise, how they synthesize the large amount of information on the topic, and the potential role of biases in their responses. Regardless of anyone's perceptions of what is actually happening and whether it will continue, decrease or increase, the fact is that vulnerabilities are constantly being discovered by both those who wish to take advantage of them and those who would like to see them managed. The time advantage goes to the offense, however, who may root undetected for months planning and laying the foundation for an exploit, where the defense must respond quickly and decisively, typically after a loss has occurred.

Insights gained over the last few years from cybersecurity specialists also reveal a disturbing blurring-of-the-lines between the capabilities of sophisticated state actors and cybercriminals who seek financial gain. Some of these commonalities include increasingly insightful use of spear-phishing emails, custom malware tools, crimeware that has been available for years, persistent presence for years and attempted return after being kicked out, and a common and growing interest in collecting PII.[551]

It is noteworthy that none of the respondents considered the ingenuity of infrastructure operators, normal emergency responses, the logical limitations of the how to combine interdependent outages of different infrastructures in their assessment. They also clearly segregated the Armageddon cyberattack from those attacks that are occurring and may yet occur within our Financial Services Sector.

The nearly coincidental dismissal of the threat of a cyber-Armageddon by the Director of National Intelligence and the prediction of an impending cyber-Armageddon by a financial regulator may ironically both be true, since so few recognize the financial services industry as an infrastructure sector, nor understand the concept and causes of systemic financial risks. Just as a few people demanding their funds from a bank may not be problem, but many of them doing so created runs on banks in the past, and just as a loss of confidence can spin out of control into a crisis of confidence, financial regulators must concern themselves with these sudden amplifications of problems within the financial services industry. They recognize the possibility that operational risks such as cybersecurity could lead to unexpected exposures or crises of confidence that institutions had not prepared for. It is this type of risk that may be most likely to lead to a cyber-Armageddon.

Scenario	Consequences	Vulnerabilities	Threats
Cyberattack leaves malware inserted in the control systems of many key infrastructures without further activation	The costs of constant scanning, cleanup and removal of malware that has not yet been used is significant but minor compared to the costs of dealing with the consequences of an actual attack that affects the operation of infrastructure. The consequences envisioned by a massive attack on key critical infrastructure are catastrophic, however, there is currently no evidence to suggest this is an imminent possibility.	Distributed nature of critical infrastructure ICS. Lack of monitoring or systems, logons, and third party vendors among utilities. Integrated nature of systems allowing less secure devices that are directly connected to the Internet to be breached, thereby granting access to the more secure ICS.	Criminal hactivists, terrorist organizations, and nation states are the most likely threat actors.

Table 31: Cyber 9/11 Scenario Type 2

The concern continues that some catastrophic attack that exploits vulnerabilities in much of U.S. physical infrastructure in a coordinated and felling strike. The reason for this continued concern is that it is common to discover that sophisticated adversaries have planted malware in systems and then just left, with a back-door to ease their access at a later date. An example of such

[551] Mandiant, M-Trends 2015: A view from the front lines, downloadable PDF at: https://www.fireeye.com/current-threats/threat-intelligence-reports.html, accessed March 17, 2015

evidence is the recent discovery that the Sony data breach and wipe, while enacted suddenly, was found to have been started a year prior.

The scale, scope, and complexity of attacks on infrastructure may be increasing, or may simply being discovered at a greater rate. The lack of clarity between the rate of occurrence and the rate of discovery is an obstacle to understanding the frequency of such attacks as well. The costs of constant scanning, cleanup and removal of malware that has not yet been used is significant but minor compared to the costs of dealing with the consequences of an actual attack that affects the operation of infrastructure. But perhaps the greatest burden associated with this “partial attack” is the realization that an adversary has invested time and resources to be ready at a moment’s notice to deliver a decisive attack. The adversary has radically changed the game, the defender has already lost, and no one really knows what may yet be discovered.

Conclusion

The risks associated with cybersecurity incidents in the U.S. are better understood today than ever before. This is a result of improved reporting and increased analytic foundations for understanding consequences. The increased transparency has provided better insight into a larger portion of a risk landscape, though it remains comparatively unclear to risk managers and planners who may try to compare these challenges to more obvious and predictable hazards, such as natural hazards, accidents, and routine crime.

Unlike natural hazards, cyberthreats do not have a geospatial aspect that makes it easier to determine the likelihood, character, or the strength of incidents. Like accidents, many cybersecurity incidents are the result of human reliability failures. Unlike accidents, cyberattacks have malicious individuals attempting to lure victims into compromising themselves.

Like routine crime, many cybersecurity incidents are all about the money. Organized crime and major drug cartels have demonstrated that having intelligent managers of a major criminal endeavor can make it all the more lucrative. This may be even more so for cybercriminal groups. Cybercriminal groups provide the opportunity to unscrupulous people who could clearly make a very respectable income in the real economy to gamble for a much more extravagant return with fairly low risk. While the prosecution of cybercrimes is increasing, the cases are so complicated, often with so many different jurisdictions involved, that it would be unreasonable to suggest that the fear of prosecution is a substantial deterrent. Like other crimes where individual’s privacy and personal autonomy is violated, there is a culture of blame and shame for the victims of cybercrime that has created a substantial incentive for victims to hide, to try to deal with these attacks privately or with the assistance of cybersecurity consultants. The degree to which this incentivizes improved security, or to which improving security can sufficiently protect an organization is unclear.

Like terrorism and Nation-state competition, failures of cybersecurity give an adversary power. This power may be in the ability to control a message, silence free speech, or deny an organization the right to do its lawful business. It may be in the ability to systematically establish and maintain a presence in our networks that allows the adversary to extract the hard-earned value of intellectual property, and turn it over to their own enterprises, so they do not have to compete on a level field. It may make it easy to figure out who works in sensitive positions and what their personal challenges are, so that intelligence agents can focus their attention on subjects most likely to become useful spies. It may be the systematic mining of the computer systems that we use to manage and operate our complex infrastructures and industrial plants with computer exploits which can be triggered at the convenience of the adversary, giving him an effective and distracting attack that may enhance some other activity. Like physical attacks by terrorists or nation-states, these politically and militarily driven cyberattacks lead to a loss of confidence in Government.

Given the diversity adversaries, their intentions, the known and unknown dangers, and the persistence of the American public in moving so much of their lives and work into cyberspace, the comparison that may be most apt is the analogy of the westward expansion of the U.S. President Barack Obama made this analogy on February 13th, 2015. He cautioned against the expectation that the U.S. could expect the Federal Government to fill the role of the sheriff in this new frontier, and he encouraged broad collaboration and cooperation across government and industry in this challenging cybersecurity space.[552]

In addition to these efforts to help stem the attacks, owners and operators of systems may be able to find ways to decouple the cause and effect of cybersecurity incidents and the harms they currently produce. Planners may be positioned to make the case for cybersecurity investments in redundancies, backups, and quick-response capabilities. Researchers in the fields of human reliability may be able to identify ways to reduce the likelihood of human errors resulting in cybersecurity compromises. Agencies may systematically identify and evaluate networks where their information is exposed, and how the exposed information could benefit adversaries, as part of their enterprise risk management. Legislators and regulators may consider how to maximize the incentives for public/private partnership on the defense of government and industry systems and services; and encourage the growth of a cybersecure workforce and public. These distributed contributions reinforce the idea that a whole-of-community approach will improve the safety and security of U.S. interests in cyberspace.

[552] National Public Radio, Obama: Cyberspace is the New ‘Wild West’, http://www.npr.org/blogs/thetwo-way/2015/02/13/385960693/obama-to-urge-companies-to-share-data-on-cyber-threats, accessed March 23, 2015.