Final Hazard Profile – Cyber Threat

"Cyber threats are no longer limited to identity theft, bank hacks or the embarrassing leak of private e-mails. It's become an all-encompassing threat that has the ability to shut down our hospitals, breach our dams and prevent the delivery of important goods to our ports. It is a matter of public safety that extends far past the borders of IT and now requires a community effort to stay ahead of those wanting to do harm." (Governor Jay Inslee in his August 19th, 2015 Letter to the Deputy Secretary of the U.S. Department of Homeland Security).

Introduction

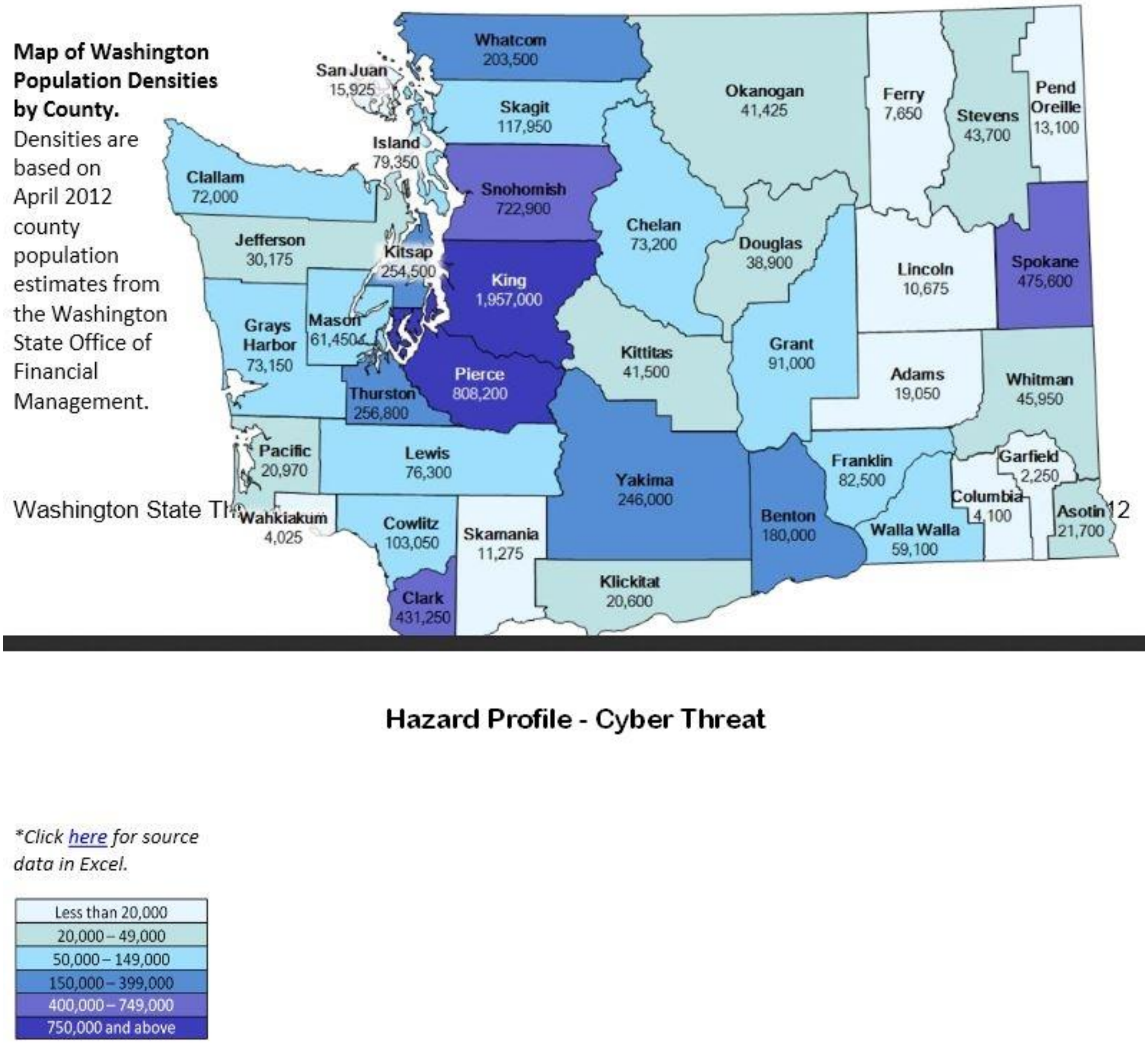
What would happen if you couldn't connect to the internet or conduct business electronically? What if all your data was lost or inaccessible? What consequences can you expect? Do you know what steps are needed to recover? These questions among others should create preemptive planning to better prepare for the cyber threat facing Washington's technological infrastructure.

Washington State is home to companies that are leading global innovation and commerce and generating billions of dollars in business. The citizens of the state depend on public and private networks for access to business, information, and essential services. In the Significant Cyber Incident Annex to the Washington State Comprehensive Emergency Management Plan (CEMP), a significant cyber incident is defined as "an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture." A significant cyber incident impacting key assets could have adverse effects which may cause harm, destruction, or loss of local and national significance (2011 National Preparedness Goal). Mitigating the cyber threat requires planning, training, collaboration and information sharing among trusted organizations.

This hazard profile is intended to provide and summarize threat information to assist planners in preparing for cyber emergencies, protecting assets, identifying vulnerabilities, anticipating damages, and protecting stakeholders. It is recommended that executive leaders and policy makers prioritize cyber emergency preparedness efforts both internally, as part of business continuity and disaster recovery efforts, and externally, working closely with community partners and emergency managers at all levels of government.

Cyber Risk Level

Frequency - Washington State ranked 10th in reported incidents of cyber crime in 2010 and 8th in 2013. Nearby states have reported seeing increased suspicious cyber activity over a 3 year span from 2 million to 20 million events per day. The frequency of nefarious cyber incidents will continue to increase especially in the more populated areas which represent the largest targets of opportunity for community disruption. A 2014 Cost of Data Breach: Global Analysis reported companies estimated an average of 17 malicious codes and 12 sustained probes monthly.



People - Approximately, 7.1 million Washington state residents depend on basic necessities and services (2014 U.S. Census Bureau estimate). Areas with higher concentrations of people and businesses are inherently more dependent on networked systems for their life sustaining services, and are therefore considered at higher risk of an emergency resulting from a significant cyber incident. A successful breach of critical public and private networks could severely diminish or destroy basic public utilities, fuel, health care systems, emergency medical services (EMS), communications, and governance to at least 50% of the population. (Calculated using counties along the I-5 corridor and counties with population over 100,000 divided by the 7.1M estimate.)

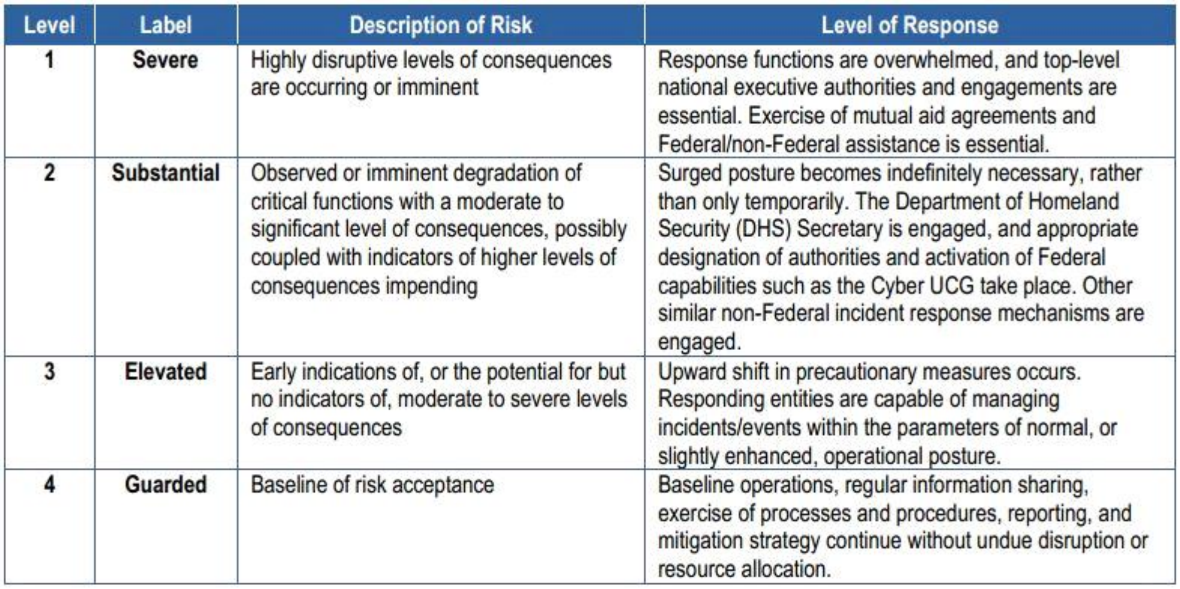
Property - The data stored on public and private networks is property in and of itself and is often the prime target of cyber criminals or lost during significant cyber outages. The most valuable data is consumer, financial, medical, intellectual property, and government information. A catastrophic incident/outage or a successful cyber-attack or breach can due untold damage. Cyber incidents can also cause physical damage to property like the December 2014 spear phishing attack on a German steel factory which disrupted the shutdown procedures for one of the plant's blast furnaces and resulted in massive damage to the plant. Another earlier example is the explosion of an oil pipeline in Turkey in 2008 which was believed to be the result of Russian hackers accessing the control systems of the pipeline and causing super pressurization. Clearly the cyber threat profile can result in both virtual and physical property damage.

Economy - The economic impact of cyber incidents depend on the size of the impacted company or community, type of attack or incident, and the physical manifestation of the network outage or disruption. Compromise of consumer information and/or financial data can severely damage the reputation of a company and due immeasurable harm to revenue generation. The loss of essential business data (Amazon) in certain sectors could shut down businesses permanently. The International Data Corporation (IDC) estimated the 2013 global loss to enterprise organizations from malware infected counterfeit software at $112 billion, nearly $350 billion in data breaches, and 1.5 billion hours lost. In a June 2014 Intel Security/McAfee report, cybercrime and espionage cost an estimated $445 billion globally which includes Microsoft Corporation. Microsoft's most current estimate is closer to $500 billion. There are no current economic estimates specifically for the state of Washington, however, Ponemon Research evaluated 257 small to enterprise level organizations around the globe to calculate the average recovery cost and expense caused by cyber breaches. Business disruption represented the highest external cost followed by information loss. Costs ranged from $567,000 for small business to $60.5 million for enterprise (Ponemon Institute, 2014 Cost of Cyber Crime Study: United States).

Environment - A significant cyber incident impacting industrial control systems such as supervisory control and data acquisition systems (commonly placed together in the acronym ICS/SCADA) that control public utilities like waste water treatment facilities or sewage processing services could cause immediate environmental and health concerns in higher population areas. Additionally, an attack on the power grid would affect nearly all basic services including the capability to heat homes, store food and/or run other critical basic life-sustaining functions. A fuel or chemical spill resulting from disruption to railway or traffic control systems could severely damage surrounding land and connected water ways irreparably for years and cost billions to cleanup.

Note: Applying total cost of a cyber incident depends on aggregated factors such as the type of data compromised, systems repaired, any financial penalties, liabilities, and reparations as well as any services like credit or identity monitoring. Total cost can't be calculated until the process is complete. Confidentiality also skews cost in some cases.

The Hazard



Level	Label	Description of Risk	Level of Response
1	**Severe**	Highly disruptive levels of consequences are occurring or imminent	Response functions are overwhelmed, and top-level national executive authorities and engagements are essential. Exercise of mutual aid agreements and Federal/non-Federal assistance is essential.
2	**Substantial**	Observed or imminent degradation of critical functions with a moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending	Surged posture becomes indefinitely necessary, rather than only temporarily. The Department of Homeland Security (DHS) Secretary is engaged, and appropriate designation of authorities and activation of Federal capabilities such as the Cyber UCG take place. Other similar non-Federal incident response mechanisms are engaged.
3	**Elevated**	Early indications of, or the potential for but no indicators of, moderate to severe levels of consequences	Upward shift in precautionary measures occurs. Responding entities are capable of managing incidents/events within the parameters of normal, or slightly enhanced, operational posture.
4	**Guarded**	Baseline of risk acceptance	Baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategy continue without undue disruption or resource allocation.

For purposes of this Hazard Profile, the cyber threat is considered a human caused technological threat, though it is acknowledged that cyber emergencies could result from the physical destruction of infrastructure during an earthquake or other natural disaster. Cyber emergencies can be caused accidentally from faults in software programming code, or deliberately by malicious hackers. The risk of coding errors occurring increases exponentially with the invention and introduction of new generations of programming languages that are purposely designed to use and reuse modules from previously written programs. Reused code may have hidden vulnerabilities. The sheer size and length of modern software programs makes it impossible to check every line of code for hazards as was the case during the March 2014 Emergency 911 outage in the pacific northwest which caused over 4500 calls to go unanswered.

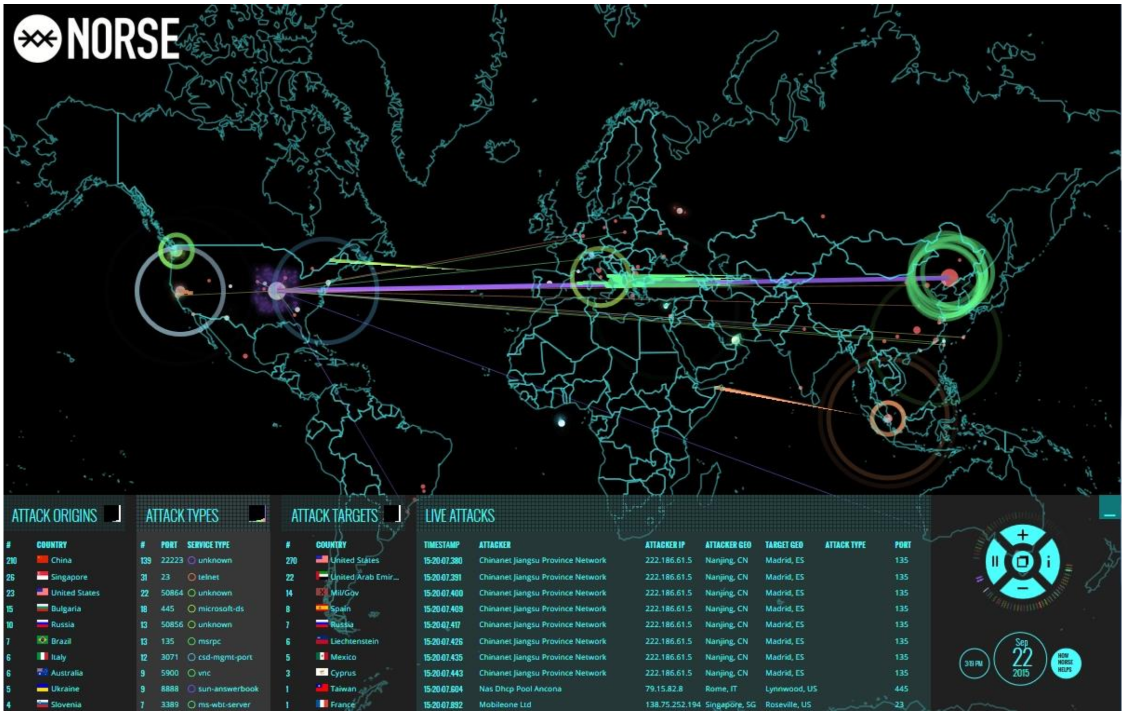
With regard to malicious actors, hackers that illegally breach systems or compromise networks do so for any number of reasons including the desire for financial gain, the challenge of breaking in to a system, political activism, terrorism, or espionage. Hackers typically attack a network through the path of least resistance which most often means through profiling, targeting, and obtaining of end-user credentials to bypass network perimeters. If the network or system can't be breached directly, hackers will look "downstream" for a vulnerable access point which may be an unsecure system on an affiliated network or application. Even if no data is taken or systems damaged, once a network has been compromised, security engineers should assume the worst till a proper assessment has been performed verifying that all systems are secure. A hacker may have simply mapped the network for future attack or shared that information with others. The threat of exploitation is so pervasive, that it is recommended that all organizations approach cybersecurity from the standpoint of "assumption of breach" and continually monitor their information systems as if they already have unauthorized users sneaking around their network.

Individual Hackers - Hackers have historically worked independently to breach targeted systems. With time and practice, hackers have improved at intrusion and moved from smaller vulnerable systems to much larger more important systems such as those belonging to business, government, or critical infrastructure service providers. The motivation of the intrusion by individual hackers may include collecting information on user accounts, theft of personal or financial information, theft of intellectual property, exploitation of sensitive company information and/or general disruption. Some individual hackers are simply motivated by the conquest of breaching a network and embarrassing the organization while fueling their own ego.

Group Hackers - Many hackers now collaborate with others to achieve their objectives. Some of these groups are called hacktivists based on apparent political motivations and/or the desire to challenge the authority, competence, and/or legitimacy of targeted organization or governments. They include idealists and radicals with a political or social agenda. The most commonly known of these hacker groups is "Anonymous", though others exist. Many of these group-affiliated hackers have limited technical skills. They often rely on purchasing and using malicious code obtained from illegal distribution websites. Working in teams strengthens their anonymity and increases the overall disruptive nature of their activities when targeted at a specific organization or agency.

Cyber Terrorism and State-Sponsored Cyber Attack - (Cyber attacks as a weapon.) A cyber terrorist goal or state-sponsored cyber attack may involve disrupting government functions, attacking Department of Defense facilities, destroying or stealing sensitive government information, disrupting critical infrastructure (as in the case of the German steel factory and the Turkish pipeline), and even causing loss of life. Some of the targeted information includes employees, staff, government contracts, and trade secrets. State backed hackers have considerable capabilities and resources at their disposal. This increases the likelihood that a network will be breached even if well protected. There are multiple documented cases of physical destruction of critical infrastructure as a result of state-sponsored cyber-attacks. Cybersecurity experts should note that both successful and unsuccessful cyber-attack information is often shared with other individuals and groups, thereby compounding the threat.

Probability of Cyber Attacks



ATTACK ORIGINS

#	COUNTRY
210	China
26	Singapore
23	United States
15	Bulgaria
10	Russia
7	Brazil
6	Italy
6	Australia
5	Ukraine
4	Slovenia

ATTACK TYPES

#	PORT	SERVICE TYPE
139	22223	○ unknown
31	23	○ telnet
22	50864	○ unknown
18	445	○ microsoft-ds
13	50856	○ unknown
13	135	○ msrpc
12	3071	○ csd-mgmt-port
9	5900	○ vnc
9	8888	○ sun-answerbook
7	3389	○ ms-wbt-server

ATTACK TARGETS

#	COUNTRY
270	United States
22	United Arab Emir...
14	Mil/Gov
8	Spain
7	Russia
6	Liechtenstein
5	Mexico
3	Cyprus
1	Taiwan
1	France

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
15-20:07.380	Chinanet Jiangsu Province Network	222.186.61.5	Nanjing, CN	Madrid, ES		135
15-20:07.391	Chinanet Jiangsu Province Network	222.186.61.5	Nanjing, CN	Madrid, ES		135
15-20:07.400	Chinanet Jiangsu Province Network	222.186.61.5	Nanjing, CN	Madrid, ES		135
15-20:07.409	Chinanet Jiangsu Province Network	222.186.61.5	Nanjing, CN	Madrid, ES		135
15-20:07.417	Chinanet Jiangsu Province Network	222.186.61.5	Nanjing, CN	Madrid, ES		135
15-20:07.426	Chinanet Jiangsu Province Network	222.186.61.5	Nanjing, CN	Madrid, ES		135
15-20:07.435	Chinanet Jiangsu Province Network	222.186.61.5	Nanjing, CN	Madrid, ES		135
15-20:07.443	Chinanet Jiangsu Province Network	222.186.61.5	Nanjing, CN	Madrid, ES		135
15-20:07.604	Nas Dhcp Pool Ancona	79.15.82.8	Rome, IT	Lynnwood, US		445
15-20:07.892	Mobileone Ltd	138.75.252.194	Singapore, SG	Roseville, US		23

Cyber-attacks and other suspicious activity are an active hourly occurrence. Washington offers a unique economic climate ideal for new business, innovation, and emerging technologies. Washington is also home to several leading industry and technology leaders. Many different international economies are linked to Washington State which increases political interest.

Taking a snapshot of internet attack activity from Norsecorp (above), on September 22, 2015 alone, Washington State received 143 direct attacks every 60 seconds. The attacks continued for several hours from various networks identified as originating from Chinese Provinces. The state economy, large cities, concentrated population centers, deep water ports, and international influence make Washington a prime target for a significant cyber incident.

Security experts should expect the cyber threat to evolve and increase. Additionally, previously disconnected or embargoed regions are joining the internet daily which increases the cyber threat not just to Washington State but to the country and its economic allies.

Attack Vectors and Definitions

There are many different attack vectors that cyber criminals can use to exploit networks. While no single vector guarantees success, some represent a serious threat for delivering a payload. Emails carrying infected software and/or malicious internet links are two common vectors for delivering malware. Through the preponderance of information obtainable through Facebook and other social media, end-users are easily profiled and targeted by hackers. These hackers easily convince end-users to open attachments in e-mails that appear to be authentic, click on embedded links, and/or provide critical information to allow for network compromise. The credentials forfeited or the malware executed by the unwitting victims is then used by the hacker to gather vital network and user information and elevate privileges for greater access. Below are common terms and methods.

Hackers	Individuals that gain unauthorized access to any private network or system. Individual hackers can leave a small virtual foot print and are often under estimated. Group hackers like hacktivists with a political or social agenda combine resources to compromise networks and systems. This collaborative effort makes them a formidable threat. Cyber terrorists are the newest cyber threat and state backed hackers with the purpose of compromising sensitive state, government, and military networks.
Malware	Malware includes Trojans, viruses, worms, scareware, and ransomware (encryption ware). Trojans are designed to trick the system by looking like legitimate software. Viruses infect and spread throughout a system often to gather information. Worms infect one or more systems throughout a network. Scareware attempts to trick users into clicking a link infected website or file. Ransomware infects and encrypts the user's storage devices exploiting payment to unlock.
DoS/DDoS	Denial of Service is an attack on a network with the goal of congesting the network or server to make it inaccessible. Distributed Denial of Service is the combined effort of using multiple systems to achieve the same. About one-third of DDoS attacks are accompanied by a network breach.

SQL/CSSX Injections	Includes but not limited to SQL injection, database exploitation, cross site scripting (CSSX), and cross site request forgery (CSRF). Each method exploits sites and databases.
Phishing	Attempts to trick users in to providing sensitive information directly or indirectly through fake websites where users unwittingly enter login credentials.
Zero-Day	This is an exploit unknown to the technology industry that allows hackers or cyber criminals to access or destroy systems or networks.
Brute Force/Exhaustive Key Search	Hackers utilize software and hardware based systems to guess and crack passwords. Methods may include a dictionary attack, password guessing, obfuscating encoded data, creating a system error, or other specialized software.
Social Engineering	Hacker method of coning or impersonating official positions in order to trick users into divulging sensitive information that can be used to compromise operation or information security.
Spoofing (Domain, DNS, Website)	Compromised data is used to poison the DNS Cache which causes the server to return a different IP address diverting traffic to the attacker's computer, server, or website. Commonly used by phishing attacks.

Other more involved intrusion methods include operating systems that come with specialized monitoring, analyzing, and mapping software. While many security experts use this software for security assessments and threat analysis, it can also be used by hackers

Some attack code like the well-known malware StuxNet, which compromised Iranian Nuclear reactor operations, poses a significant threat to critical infrastructure in particular. StuxNet was a customizable worm that was created specifically to target, damage, and destroy uniquely identified programmable logic controllers used by the Iranian Nuclear Reactor SCADA systems. In the case of StuxNet, the malware was created as a “logic bomb” that remained dormant until entered onto the target network where a specific piece of program logic activated it within the SCADA system. Logic bombs are designed for specific systems and triggered by the unique functions of that system. StuxNet attacked the nuclear centrifuges and undermined the Iranian nuclear program successfully for more than a year. StuxNet is believed to be in the hands of coders and may have moved to unknown networks on the internet.

Another StuxNet variant named Duqu, shares similar code that records keystrokes and other system information. Duqu's purpose is thought to be more about reconnaissance used possibly for a future attack (Symantec).

Flame, or Skywiper, is essentially modular malware used for targeted cyber espionage. After the confidential information has been acquired, a "kill" command can be sent wiping all traces of itself from the infected system(s). While originally found in Middle Eastern countries, Flame has been found in Europe and North America. There are nine other known variations of malware code created from Flame.

History of Attacks

Anticipating what hackers will use and why is particularly difficult. In most cases, hackers want to exploit or destroy data. In other cases, the hackers want to control or destroy systems. However, understanding the history of attacks and the value of targets to threat actors can help security experts develop planning and policy. In general, commercial and financial systems have a higher rate of monetary return while government systems are often targeted for information exploitation and disruption activities.

Pranks and Hacks

A low level attack consisting of "taking a peek" at systems or having a little online fun can create havoc for security personnel. In the last few years, hackers compromised Montana and Michigan Emergency Alert Systems (EAS) to broadcast a message saying zombies were attacking. The messages were heard on radio and television stations. While the result was relatively harmless, the ability to take over the EAS is of grave concern. A more plausible message could confuse first responders and cause public panic.

In a more serious case of hacking, an Indianapolis 911 system was taken offline by hackers which fortunately came back online thanks to redundant systems. In the wake of public reaction to the Ferguson, Missouri police shootings, hacktivists defaced government websites, researched and broadcasted personal information about public officials (an activity known as Doxxing), and further targeted and smeared public officials with false information over the internet. Further activities included the compromise of 911 systems preventing emergency responders from receiving calls for several hours.

Human and System Error

Human and system error can undermine key enterprise strategies. Mismanaged servers, end of life software, unmanaged devices and unpatched applications can cause system failures and also create back door vulnerabilities. A hacker could potentially remote connect; upload malware, change privileges, and compromise data among many other damaging actions.

In 2003, a power company representative unintentionally executed malware resulting in power outages for the Northeastern U.S. and parts of Canada. The malware was designed to infect Windows systems and inadvertently affected Unix servers, disrupting the power grid across multiple states. The vulnerability was unknown to security administrators making it a trifecta example of human error, system error, and an unintended "zero-day" exploit. A zero-day exploit means the vulnerability was unknown and unpatched within the operating systems.

Most of Washington State and other areas around the United States experienced a 6-hour 911 phone system outage due to human error in 2014 resulting in some 4500 unanswered calls. Redundant systems failed to function as designed at a processing facility in Colorado. The outage was the result of a vulnerability discovered in the design of the software that controlled the system. Fortunately, no lives were lost.

Social engineering by hackers is the targeting of specific end-users or a group of end-users, and using all the information available via social media or other methods (false solicitation phone call, etc) to convince the targeted person(s) to click on something or provide some key piece of information that will allow the hacker to enter the network. Avoiding fake websites and spotting phishing tactics is the responsibility of every computer operator and is perhaps the biggest challenge for information security professionals.

The health insurer Anthem and Premera Blue Cross were both compromised by hackers who created a fake website and an exploit called Domain Spoofing. Members unwittingly attempted to login to the fake website with legitimate credentials. A combined total of close to 100 million internal and external members' personal data was compromised. If such attacks are not properly investigated, the process can be replicated and even shared with other hackers. These attacks have cost both companies hundreds of millions of dollars in labor, equipment and credit monitoring services for their customers, and done immeasurable damage to their reputations.

Hacktivism

Hacktivists, or hackers with a cause, have the goal of compromising public and private networks using the same tools as any hacker in order to carry out political or idealistic objectives. Regardless of purpose, bringing down essential state and government services only makes it more difficult to assist citizens in need.

The hackers that carried out a DDoS attack on EMS and local government offices/personnel (Ferguson, Missouri, Aug 2014) are commonly referred to as hacktivists that operated under the guise of "Anonymous". In this example, the constant disruption caused by hacktivists to communications and public officials most certainly caused delays/distractions in the general public receiving emergency assistance.

A Muslim hacktivist group named Cyber Fighters of Izz-ad-din Al Qassam mounted DDoS attacks against U.S. banks in retaliation after a Muslim film was posted on Youtube. The cyber-attack came in three phases. U.S. intelligence reported that the hacktivist group was backed by the Iranian government.

Global hacktivism can have more adverse effects on the United States. Some political hacktivists have demonstrated the ability to undermine government security by spamming, defacing websites, inserting malware, phishing and perpetrating denial of service (DoS/DDoS) attacks. In 2011, the Syrian Electronic Army carried out such attacks against various governments and organizations. With Syrian government support, the SEA is among the most serious threats.

National Security

The United States government, military, and affiliated networks are all prime targets for national and international hackers. Collaborative Chinese hackers probed and are alleged to have stolen sensitive data over an undisclosed amount of time from government contractors (Lockheed Martin and Northup Grumman) over the two year development phase of the F35 Joint Strike Fighter. Similar hackers were also responsible for the largest data breach of federal employee information from the Office of Personnel Management. While personal information may have been the primary target, the information gathered could compromise operations and other connected networks.

In April 2015, Deputy National Security Adviser Ben Rhodes confirmed that Russian hackers compromised a non-classified system over a several month period to obtain information about the President's activities. The hackers accessed the White House systems "downstream" via the State Department using login credentials gained through spear phishing.

As mentioned briefly above, a July 2015 incident revealed that as many as 22.1 million government employees, contractors, and other personnel records stored within the U.S. Office of Personnel Management were compromised by a cyber-attack traced back to networks managed by the Chinese government. The FBI stated this was of serious cyber security and national security importance given the information can be used for counterintelligence purposes.

ICS/SCADA/DCS/PLC

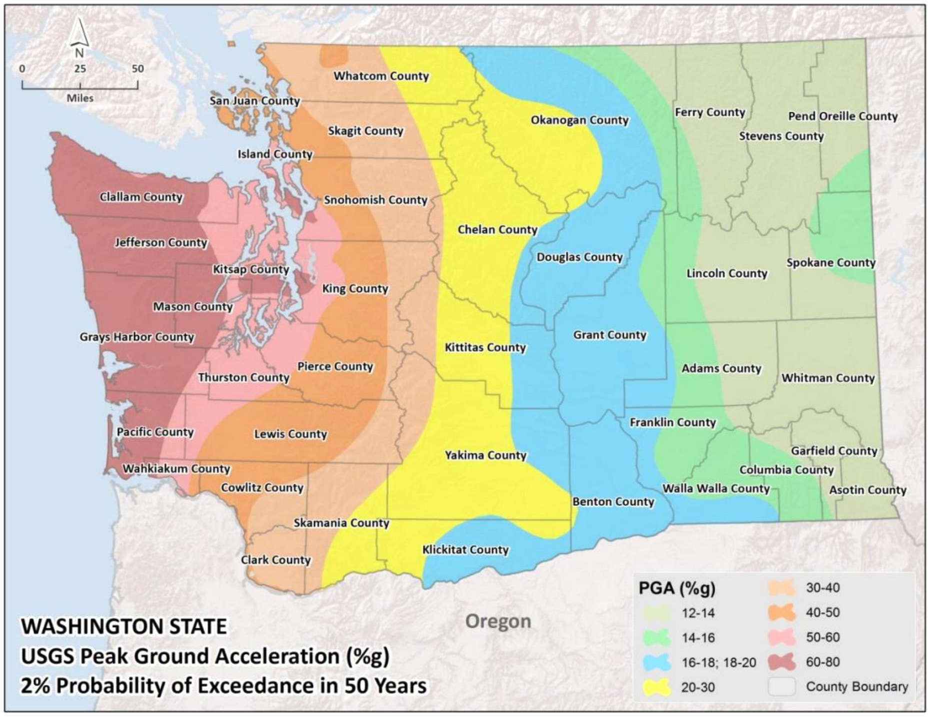
In Washington State alone, roughly 7.2 (2015) million citizens depend on utilities and services. ICS are used to manage industries such as electric, water and wastewater, oil and natural gas, transportation, ports of call, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing. ICS utilizes SCADA systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC).

Hackers target these systems mainly to disrupt damage and destroy services. If the cyber-attack succeeds, the result can include wide area service outages, disrupt power and water, create chaos for transportation, and create infrastructure security issues. Depending on the cyber attack, a disruption to one or more utilities and essential services could last for several days.

As previously noted, a Windows targeted malware caused unforeseen vulnerabilities and side effects in UNIX systems used to control the power grid in the Northeast U.S. and parts of Canada in 2003. In a financially related example, Trendmicro found 13 different types of malware disguised as banking malware that were in fact created to attack ICS/SCADA systems.

Internationally, hackers were able to shut down Saudi owned ARAMCO and Iran refineries using various customized viruses. In a more destructive instance referred to previously, hackers disabled alarms, communications and caused a crude oil refinery on the Turkish pipeline (Turkey Aug 5, 2008) to explode destroying operations and facilities costing millions in loss of property and oil.

Disaster



Immediately after a physical disaster such as an earthquake or volcano eruption, response personnel will be focused on immediate life-saving efforts. Critical network systems will be especially vulnerable to exploitation and attack by nation-states, terrorist groups, organized crime elements, hacktivists, etc., while community attention is focused on disaster response. With one or more resource, emergency, or state managed networks partially or completely offline, devices responsible for security may also be unable to detect intrusion. Security administrators may not be able to access their networks or devices due to local or regional disconnects making securing these systems impossible. During this vulnerable period, security engineers should collaborate to mitigate potential security risks. As soon as is practicable, technical personnel should be called upon to secure networked systems from opportunistic exploitation.

Infrastructure

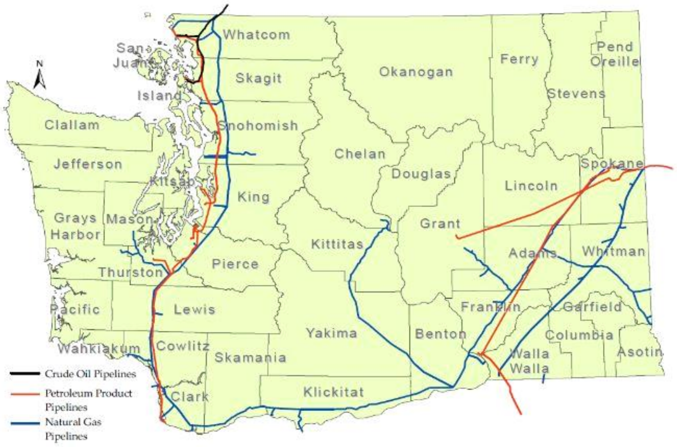


Figure 1: Washington State Pipeline Distribution Network. The location of pipelines responsible for carrying natural gas, petroleum products (including jet fuel, gasoline, etc.), and crude oil located with Washington State.

Cyber criminals, terrorists and hackers with a great deal to gain will find other avenues to compromise and disrupt transportation, essential services, and communications by physically attacking weak or vulnerable locations. Large information producing areas with hubs, street vaults housing data lines, major communications, and gas/oil lines are just some of the physical infrastructure targets. Without proper physical security, a bolt cutter may be all that is needed to gain access and create serious disruption which will put lives at risk. Depending on the infrastructure impacted, a cyber-attack or incident could conceivably result in large scale outages, destroyed systems, prevent critical services and systems from being affective, and hamper the ability to distribute goods and services. This in and of itself could be the origin of a disaster resulting in loss of life and civil unrest resulting from a loss of citizen confidence in government.

Meeting the Threat

"[Cybersecurity] is a matter of public safety and national security… The cyber threat is one of the most serious economic and national security challenges we face as a nation." (President Obama 2009)

Information technology continues advancing at a considerable pace, increasing the need for better collaboration and growth of a work force ready to meet the cyber threat. However, there are enduring external and internal obstacles. Policy and trust challenges between agencies and businesses often prevent open sharing of cyber threat information. Too often organizations worry that revealing cyber-attack information and their own vulnerabilities could reduce their competitive edge in the market and/or damage their own credibility. To the extent possible within legal and regulatory boundaries, communities must strive to develop public/private sector information sharing organizations with charters to protect the identities of reporting organizations. Reported incidents should be used as learning and training opportunities to improve collective skills and create cohesive cyber security programs throughout the communities of interest.

Washington State and federal planning efforts for the cyber threat profile intersects through the core capability-based, Washington State Threat and Hazard Identification and Risk Assessment (THIRA). The THIRA methodology includes a significant cyber incident scenario that overwhelms the response capabilities of the agency(s) impacted and threatens the safety and security of our citizens, and a corresponding set of desired outcomes and capability targets. These scenario-based targets provide a platform against which the state assesses its planning, organization, equipment, training and exercise capabilities for the annual State Preparedness Report. The capability targets and gap assessments then provide a framework for strategic planning to fill the gaps.

FEMA considers the Cybersecurity core capability to be a Protection Mission Area capability, with an emphasis on early detection to ward off significant incidents. Washington State has determined the Cybersecurity capability to cross all five mission areas of Prevention, Protection, Mitigation, Response and Recovery. As such, over time the state THIRA will include scenario-based impacts, targets and strategic objectives to cover all phases of cyber incident planning.

Cyber Threat Summary

The cyber threat to Washington State residents, businesses, infrastructure, and public agencies is very real and increasing every day. A significant cyber incident could create considerable challenges for 7.1 million citizens that depend on networked systems for commerce, utilities, and countless essential services. Preparing for and responding to cyber emergencies far exceeds the capabilities of information technology professionals and their organizations alone, and must be embraced holistically by every citizen, employee, manager, and executive from all sectors. Washington business and government leaders should continue to develop and improve planning and preparation for a significant cyber incident. With the direct support of their executive leadership, key personnel like emergency managers, business continuity officers, IT security professionals, and public safety officials throughout the community must continue to develop emergency response plans, conduct exercise and training activities, and share cyber threat information. This Hazard Profile was published to assist these critical offices in understanding the threat in order to better prepare for the impending cyber emergencies we will face as a state.

This report was prepared by Eric Garay, Cybersecurity and Forensics Engineer, Highline College with assistance from Matt Modarelli, Cyber Security Manager, Washington State Emergency Management Division, and review by LTC Thomas Muehleisen, Cyber Policy, Washington National Guard J-36.

REFERENCES

Washington State Cyber Security Program

http://mil.wa.gov/emergency-management-division/cyber-security-program

The Comprehensive National Cybersecurity Initiative

https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Community Cyber Security Maturity Model (CCSMM)

The mission should be to obtain the Vanguard cyber posture. Continued training through collaboration and education.

DHL: Responding Quickly to Cyber Vulnerabilities

By maintaining a team of skilled cyber security professionals and partnering with the private sector, DHS has been able to effectively respond to cyber incidents; provide technical assistance to owners and operators of critical infrastructure and disseminate timely and actionable notifications regarding current and potential security threats and vulnerabilities.

Sources and Citations

Introduction Resources

Senator Carper Introduces Bill to Increase Sharing of Cyber Threat Data. (2015, February 11). Retrieved June 1, 2015, from http://www.carper.senate.gov/public/index.cfm/2015/2/senator-carper-introduces-bill-to-increase-sharing-of-cyber-threat-data

U.S. Congress. (2014, July 10). To Improve Cybersecurity in the United States; Enhanced Sharing of Information. Retrieved June 1, 2015, from https://www.congress.gov/bill/113th-congress/senate-bill/2588

Ruppersberger, D. (2015, January 8). U.S. Congress, Cyber Intelligence Sharing and Protection Act H.R. 234. Retrieved June 1, 2015, from https://www.congress.gov/bill/114th-congress/house-bill/234 - H.R.234

Carper, T. (2015, February 11). U.S. Congress, Cyber Threat Sharing Act of 2015. Retrieved October 4, 2015, from https://www.congress.gov/bill/114th-congress/senate-bill/456/all-info

Clapper, J. (2015, February 26). Office of the Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community. Retrieved June 1, 2015, from http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Prevention Resources

National Cyber Incident Response Plan. (2010, September 1). Retrieved June 5, 2015, from http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf

Current Activity Web Page. (n.d.). Retrieved June 5, 2015, from https://www.us-cert.gov/ncas/current-activity

Frequency

Cawley, D. (2013, February 20). State Faces Millions of Cyber Attacks Per Day. Retrieved June 5, 2015, from http://www.ksl.com/?nid=148&sid=24141005

Tomaso, M. (2013, March 6). BP Fights Off Up to 50,000 Cyber-Attacks a Day. Retrieved June 5, 2015, from http://www.cnbc.com/id/100529483

Press, A. (2013, March 6). Michigan Fends Off 187,000 Cyber-Attacks A Day. Retrieved June 5, 2015, from http://www.crainsdetroit.com/article/20130306/NEWS01/130309926/michigan-government-spends-millions-on-cybersecurity

Stop Think Connect - Government Tip Card. (2013). Retrieved June 5, 2015, from http://www.dhs.gov/sites/default/files/publications/Government-Tip-Card.pdf

Stinson, J. (2014, October 2). Cyber-Attacks on State Databases Escalate. Retrieved June 5, 2015, from http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/10/02/cyberattacks-on-state-databases-escalate

Wilshusen, G. (2013, March 7). A Better Define d and Implemented National Strategy Is Needed to Address Persistent Challenges. Retrieved June 5, 2015, from http://www.gao.gov/assets/660/652817.pdf

http://www.craveninsurance.com/2014/12/washington-state-cyber-liability-trends - 39% of Small Businesses like Whidbey Island and Lake Stevens Experience Cyber Incidents

Economy

Chaput, M. (2015, March 24). Calculating the Colossal Cost of a Data Breach. Retrieved June 5, 2015, from http://ww2.cfo.com/data-security/2015/03/calculating-colossal-cost-data-breach/

Ponemon Institute, 2014 Cost of Data Breach: Global Analysis. Retrieved July 14, 2015, from http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis - 2014 Cost of Data Breach: Global Analysis

Digital Detectives, Cybercrime Statistics. Retrieved September 12, 2015, from https://news.microsoft.com/stories/cybercrime/index.HTML

Ponemon Institute, 2014 Cost of Data Breach: United States. Retrieved July 15, 2015, from http://www.ponemon.org/library/2014-cost-of-data-breach-united-states?s=2014+cost+of+data+breach

Ponemon Institute, 2014 Cost of Global Data Breach: Global. Retrieved July 14, 2015, from http://www.ponemon.org/library/2014-cost-of-data-breach-global?s=2014+cost+of+data+breach

People

McAffee and Intel Security (2014, June), McAfee Net Losses: Estimating the Global Cost of Cybercrime. Retrieved July 12, 2015, from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf - 2014

United States Census Bureau (2015, September 30), Washington State Census Statistics. Retrieved July 1, 2015, from http://quickfacts.census.gov/qfd/states/53000.html

Property

Microsoft APAC News Center (2015, February 16), Microsoft Launches Cybercrime Satellite Centre to Advance Cybersecurity in Singapore and Asia Pacific. Retrieved September 10, 2015, from https://news.microsoft.com/apac/2015/02/16/microsoft-launches-cybercrime-satellite-centre-to-advance-cybersecurity-in-singapore-and-asia-pacific/

Microsoft News Center (2013, March 6), Software Piracy Costs Billions in Time, Money for Consumers and Businesses. Retrieved March 5, 2013, from https://news.microsoft.com/2013/03/06/software-piracy-costs-billions-in-time-money-for-consumers-and-businesses/

The IP Commission Report (2013, May), The Report of The Commission on the Theft of American Intellectual Property. Retrieved July 12, 2015, from (http://www.ipcommission.org/report/ip_commission_report_052213.pdf -

Jennifer Warnick (2014), Microsoft Cybercrime Digital Detectives. Retrieved August 10, 2015, from https://news.microsoft.com/stories/cybercrime/index.HTML

Kacper Pempel (2014, June 9), Cyber Crime Costs Global Economy $445 Billion a Year: Report. Retrieved Aug 10, 2015, from http://www.reuters.com/article/2014/06/09/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609

Committee on Energy and Commerce (2013, July 9), House Hearing CYBER ESPIONAGE AND THE THEFT OF U.S. INTELLECTUAL PROPERTY AND TECHNOLOGY. Retrieved July 21, 2015, from 2013http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm

http://www.itworld.com/article/2861675/cyberattack-on-german-steel-factory-causes-massive-damage.html

http://www.slate.com/blogs/future_tense/2014/12/11/bloomberg_reports_a_cyber_attack_may_have_made_a_turkish_oil_pipeline_catch.html

Hacks and Pranks

The Associated Press (2014, August 13), Hackers cause problems for police computers in Ferguson. Retrieved July 14, 2015, from http://www.kmbc.com/news/hackers-cause-problems-for-police-computers-in-ferguson/27460828 - Hackers Cause Problems for Police Computers in Ferguson (MO)

Mathew Schartz (2013, February 12), Zombie Alert Hoax: Emergency Broadcast System Hacked. Retrieved July 15, 2015, from http://www.darkreading.com/attacks-and-breaches/zombie-alert-hoax-emergency-broadcast-system-hacked/d/d-id/1108621?

Upper Michigans Source (2013, February 11), Zombies? Emergency Broadcast System Hacked. Retrieved August 30, 2015, from http://uppermichiganssource.com/news/local/zombies-emergency-broadcast-system-hacked?id=859352#.URqI4h2Cmuk

Jeremy Brilliant (2015, February 16), Hackers Target Indianapolis 911 Center. Retrieved August 16, 2015, from http://www.wthr.com/story/27897557/hackers-target-indianapolis-911-center - Hackers Target Indianapolis 911

http://www.urbandictionary.com/define.php?term=doxxing

Human and System Error

Robert Ackerman (2013, July 31), SCADA Systems Face Diverse Software Attack Threats. Retrieved July 18, 2013, from http://www.afcea.org/content/?q=scada-systems-face-diverse-software-attack-threats

Suzanne Deffree (2015, August 14), Northeast Blackout Leaves 50M People Without Power. Retrieved August 16, 2015, from http://www.edn.com/electronics-blogs/edn-moments/4394019/Northeast-blackout-leaves-50M-people-without-power--August-14--2003

Bruce Schneier (2008, June 2), Did the Chinese PLA Attack the U.S. Power Grid?. Retrieved August 25, 2015, from https://www.schneier.com/blog/archives/2008/06/did_the_chinese.html

Jeremy Kirk (2015, March 18), Premera, Anthem data breaches linked by similar hacking tactics (Domain Spoofing). Retrieved August 21, 2015, from http://www.computerworld.com/article/2898419/data-breach/premera-anthem-data-breaches-linked-by-similar-hacking-tactics.html - Premera Anthem Domain Spoofing Hack

BeyondTrust Research Team (2015, March 18), Premera Breach – What Happened and Was it Related to the Anthem Breach?. Retrieved August 28, 2015, from http://blog.beyondtrust.com/premera-breach-what-happened-and-was-it-related-to-the-anthem-breach - Anthem Breach

Hacktivism

Trend Micro: Security News (2015, August 17), Hacktivism 101: A Brief History and Timeline of Notable Incidents. Retrieved September 10, 2015, from http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/hacktivism-101-a-brief-history-of-notable-incidents

KrebsonSecurity (2014, June 13), Iranian Elections Bring Lull in Bank Attacks. Retrieved August 14, 2015, from http://krebsonsecurity.com/tag/izz-ad-din-al-qassam-cyber-fighters/

Tracy Kitten (2013, July 23), DDoS: Attackers Announce Phase 4. Retrieved July 25, 2015, from http://www.bankinfosecurity.com/ddos-attackers-announce-phase-4-a-5929/op-1

CBS SF Bay Area (2014, December 1), Sony's Computer System Hacked, Causing Problems For Film Studio. Retrieved July 25, 2015, from http://sanfrancisco.cbslocal.com/2014/12/01/sonys-computer-system-hacked-causing-problems-for-film-studio - Hackers Cause Sony Major Financial, Reputational Damage

Tara Seals (2015, September 17), One-Third of DDoS Attacks Accompanied by Network Breach. Retrieved September 24, 2015, from http://www.infosecurity-magazine.com/news/one-third-of-ddos-attacks-network

ICS/SCADA/DCS/PLC

Patrick Kiger (2013, October 25), 'American Blackout': Four Major Real-Life Threats to the Electric Grid. Retrieved August 20, 2015, from http://energyblog.nationalgeographic.com/2013/10/25/american-blackout-four-major-real-life-threats-to-the-electric-grid/

Trend Micro: Security News (2015, August 17), Hacktivism 101: A Brief History and Timeline of Notable Incidents. Retrieved September 10, 2015, from http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/hacktivism-101-a-brief-history-of-notable-incidents

Robert Ackerman (2013, July 31), SCADA Systems Face Diverse Software Attack Threats. Retrieved July 18, 2013, from http://www.afcea.org/content/?q=scada-systems-face-diverse-software-attack-threats

Danielle Veluz (2010, October 1), STUXNET Malware Targets SCADA Systems. Retrieved August 10, 2015, from http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems

Darlene Storm (2014, January 15), Hackers exploit SCADA holes to take full control of critical infrastructure. Retrieved July 26, 2015, from http://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical-infrastructure.html

SCADAhacker (2015), Vulnerability Trend Data. Retrieved July 24, 2015, from https://www.scadahacker.com/resources.html

http://resources.infosecinstitute.com/scada-security-of-critical-infrastructures/ - SCADA & Security of Critical Infrastructure

Robert Ackerman (2013, June 1), Critical Infrastructure Ripe for Attack, (Saudi Aramco Hacked, South Korean Banking Trojans Infect SCADA). Retrieved August 12, 2015, from http://www.afcea.org/content/?q=node/11120

Kelly Higgins (2015, January 8), Banking Trojans Disguised As ICS/SCADA Software Infecting Plants. Retrieved August 10, 2015, from http://www.darkreading.com/attacks-breaches/banking-trojans-disguised-as-ics-scada-software-infecting-plants/d/d-id/1318542

(Image) Columbia Nuclear Power Station, Retrieved September 21, 2015, from http://energy.gov/ne/nuclear-reactor-technologies

(Image) Map of National Nuclear Power Stations, Retrieved September 21, 2015, from http://www.nrc.gov/reactors/operating/map-power-reactors.html

Mandiant (Feb 2014), APT1 Exposing One of China's Cyber Espionage Units. Retrieved July 26, 2015, from http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Ariel Bogle (2014, December 11), A Cyber Attack May Have Caused a Turkish Oil Pipeline to Catch Fire in 2008. Retrieved July 5, 2015, from http://www.slate.com/blogs/future_tense/2014/12/11/bloomberg_reports_a_cyber_attack_may_have_made_a_turkish_oil_pipeline_catch.html

National Security

Ellen Nakashima (2015, July 9), Hacks of OPM Databases Compromised 22.1 Million People. Retrieved August 21, 2015, from http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/

Danielle Veluz (2010, October 1), STUXNET Malware Targets SCADA Systems. Retrieved August 10, 2015, from http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems

Kristen Echensehr (2015, March 6), Cybersecurity in the Intelligence Community’s 2015 Worldwide Threat Assessment. Retrieved August 25, 2015, from http://justsecurity.org/20773/cybersecurity-u-s-intelligence-communitys-2015-worldwide-threat-assessment/

Jason Koebler (2012, March 20), U.S. Nukes Face Up to 10 Million Cyber Attacks Daily. Retrieved July 25, 2015, from http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily - 10 Million Daily Cyber Attacks Daily at Nuclear Security Enterprise, Nat'l Nuclear Security Administration

Attack Vectors and Definitions

Tara Seals (2015, September 17), One-Third of DDoS Attacks Accompanied by Network Breach. Retrieved September 24, 2015, from http://www.infosecurity-magazine.com/news/one-third-of-ddos-attacks-network

DNSCurve (2006, June 24), DNSCurve: Usable security for DNS. Retrieved July 24, 2015, from http://dnscurve.org/forgery.html - DNS Spoofing/Forgery

Laboratory of Cryptography and System Security (2011, October 14), Duqu: A Stuxnet-like malware found in the wild. Retrieved September 29, 2015, from http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf - Duqu: A Stuxnet-like malware found in the wild

Laboratory of Cryptography and System Security (2012, May 31), Skywiper (Flame or Flamer) A Complex Malware for Targeted Attacks. Retrived September 29, 2015, from http://www.crysys.hu/skywiper/skywiper.pdf - Flame/Skywiper - Nine Versions of Flame/Skywiper

Get Cyber Safe (2015). Retrieved July 23, 2015, from http://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-eng.aspx

Cybersecurity Awareness (2015), Common Cyber Threat Indicators and Countermeasures. Retrieved July 23, 2015, from http://cdsetrain.dtic.mil/cybersecurity/data/pdf/Common_Cyber_Threats_Indicators_and_Countermeasures.pdf

Symantec-Norton (2015). Retrieved July 24, 2015, from http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx

http://www.tech-faq.com/logic-bomb.html