3.12: Cyberterrorism Risk Assessment

Hazard Description

A cyber-attack is a malicious, intentional attempt to breach the information technology (IT) infrastructure of an individual or organization. The State of Mississippi defines a cyberterrorism incident as any adverse premeditated, politically, financially, or maliciously motivated attack against information systems. A cyberterrorism event can impact one or more State or local government departments and divisions' information assets in the following ways:

- Unauthorized use
- Malicious coding
- Application system failures
- Security breaches
- Backdoor trojans
- Malware
- Denial of service
- Network system failures
- Loss of data
- Injection of Structured Query Language (SQL)
- Phishing
- Ransomware

Incidents often target specific types of data including:

- Financial data
- Databases
- Login credentials
- IT services
- Client or constituent lists
- Email addresses
- IT Infrastructure
- Personal data

The motives behind cyberterrorism attacks can vary. Some of the motives behind cyber attacks may include:

- To make a political or social point
- For the intellectual challenge
- Cyberwarfare
- Financial gain
- To gain a (business) advantage
- Revenge

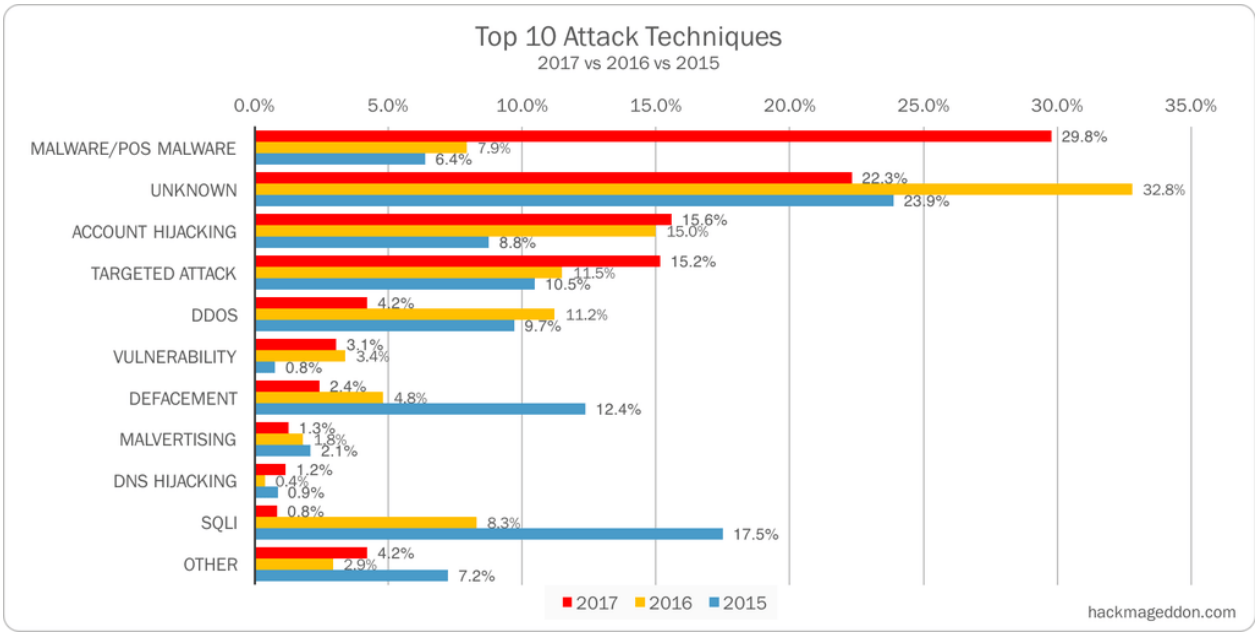
Hazard Profile

The U.S. Department of Homeland Security identifies cyber incidents in two broad categories including data breaches and physical infrastructure failures. Both categories represent the potential for vulnerabilities to essential financial, communications, information, and security systems. A data breach includes any situation including those listed above, in which a person, organization, or agency gains unauthorized or illegal access to personal, sensitive, or confidential information. A cyber-induced physical infrastructure failure could disable multiple essential functions, isolating communities and restricting access to energy, food, clean water, and other emergency services.

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. CISA Region 4 includes Alabama, Florida,

Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee and provides support, preparation, response, and recovery efforts for hazards impacting critical infrastructure in those states.

Figure 3.11.3
Top 10 Techniques



Source: *Hackmageddon.com*

Location and Extent

The cyberterrorism hazard is not geography-based. Attacks can originate from any computer to affect any other computer in the world. If a system is connected to the Internet or operating on a wireless frequency, it is susceptible to exploitation. Targets of cyberterrorism can be individual computers, networks, organizations, business sectors, or governments. Financial institutions and retailers are often targeted to extract personal and financial data that can be used to steal money from individuals and banks.

When a cyber security incident occurs, the State of Mississippi's Office of Homeland Security uses the following factors to evaluate its severity:

- Nature of the attack
- Criticality of systems that are (or could be) made unavailable
- Value of the information compromised (if any)
- Number of people, agencies, or functions impacted
- Business considerations
- Public relations
- Effects on the State's entire IT enterprise

Cyberterrorism may range from the infection of a single machine by a common computer virus to a large-scale, organized incident that cripples an organization or infrastructure.

Previous Occurrences

Even though there has been no disruption of services within the State government, Mississippi is no stranger to similar types of cyberterrorism attacks. In 2017, a Lebanese national executed a distributed denial of service (DDOS) attack on a Ridgeland business. The hacker utilized a computer in Lebanon to extort payments from the Ridgeland business while conducting computer attacks to interfere with its computer business and operations. This type of act is considered a denial-of-service attack, where an attacker attempts to prevent legitimate users from accessing information or services, preventing one from accessing email, websites, online accounts (banking, etc.), or other services that rely on the affected computer.

Even as this plan is being updated, the City of Atlanta has been held hostage by a ransomware attack for 6 days and counting. So far, the hackers are asking $51,000 in Bitcoin to unlock the city's systems. Luckily, emergency services such as 911 calls and control of wastewater treatment have been exempt from the attack.

To date, most experts believe this is one of the most sustained, coordinated, and consequential cyberterrorism attacks ever mounted against a major American city. The assault on Atlanta, the core of a metropolitan area of about 6 million people, represented a serious escalation from other recent cyberattacks on American cities, like the one last year in Dallas where hackers gained the ability to set off tornado sirens in the middle of the night.

Actions are taken by the Department of Information Technology Services to mitigate security risks presented by, for example, blocking IP address ranges, identifying vulnerable servers, performing scans as necessary, opening Help Desk tickets to scan/check machines, etc. Losses can include loss of productivity, financial theft, and the exposure of secure information. To date, no specific losses from cyberterrorism that have affected the State are available.

Probability of Future Occurrences

As is the case for any large governmental organization, the State of Mississippi will continue to be impacted and compelled to respond to cyberterrorism in the future. The nature of these attacks is projected to evolve in sophistication over time. The State has taken a proactive position in its cyber security efforts and is expected to remain vigilant in its efforts to prevent attacks from occurring and/or disrupting business operations. The reality remains that many computers and networks in organizations of all sizes and industries around the United States will continue to suffer intrusion attempts daily from viruses and malware that are passed through websites and emails.

Vulnerability Assessment

To understand risk, the State will continue to evaluate what assets are exposed or vulnerable in the identified hazard area. For the cyberterrorism hazard, the entire State of Mississippi is exposed to this hazard. Therefore, all assets in the State (population, structures, critical facilities, and lifelines), as described in the State's profile section are exposed and potentially vulnerable to a cyberterrorism attack.

Because it is difficult to predict targets of cyberterrorism, assessing vulnerability to the hazard is also difficult. All populations who directly use a computer or those receiving services from automated systems are vulnerable to cyberterrorism. Although all individuals in the State of Mississippi are vulnerable to an attack, certain types of attacks would impact specific segments of the population. If the cyberterrorism attack were to target the State's power or utility grid, individuals with medical needs would be impacted the greatest. Unfortunately, these populations are most vulnerable because many of the life-saving systems they rely on require power. Also, if an attack occurred during months of extreme heat or winter weather, the State's elderly population (those 65 years of age and older) would be vulnerable to the effects of the lack of climate control. These individuals would require shelter or admission to a hospital.