Cyber Threats in U.S. California

Maame Darko

Old Dominion University

CYSE/POLS 526 Cyber War

Final Project Paper

April 10th, 2024

Cyber Threats in U.S. California

Introduction

Cyber threat is a malicious action performed by an attacker to steal or destroy confidential information, data, or the whole wellbeing of a device. It is any criminal act with the intention to cause harm to a personal or organizational device and intellectual properties. Cyber threats can come from anywhere in the world, within the organization or remotely and from anyone including trusted users and unknown external parties. California, as a major global technology and innovation center, has enormous digital networks and systems in place. This makes it an appealing target for criminals attempting to take advantage of whatever vulnerabilities they might discover. These cybercriminals may attempt to get access to sensitive information, disrupt services, or cause other harm for monetary gain or malicious intent. This demonstrates why cyber threats should be a top concern for Californians and organizations in California.

Overview

This paper will describe cyberthreats and outline California's concerns about them. It will also examine various cyberthreats and their impact on the state. Then investigate the weaknesses in the networks and systems of California. Lastly, it will cover the steps being taken to defend against these threats and possible advances for cybersecurity in California.

Types of Cyber threats

Cyber Threats in U.S. California

Cyber threats can take many different forms, creating complex problems that require constant attention to detail and innovative solutions for resolution. Some of them are as follows.

- Malware attacks - A malware attack is a common cyberattack that involves the execution of unauthorized actions or performances on an individual or organizations systems by malicious software. The malicious software is normally referred to as a virus. It consists of many types of attacks such as spyware, ransomware, adware, trojans, rootkits, worms, and files malware.

- Phishing scams - Phishing is a cyber threat/cybercrime in which targets are reached through phone calls (vishing), emails, text messages (smishing), by the attacker acting as a certain company, asking for confidential information such as credit card number, social security number or password, under false pretenses, with the malicious intention of exploitation.

- DDoS attacks - DDoS attacks occur when numerous computers send traffic to a website or online service, overloading it." As a result, the system gets overwhelmed and inaccessible to regular users. DDoS attacks are frequently used by hackers to take down websites or demand money from organizations.

- Spoofing - Spoofing attacks include masking communications or identities so that they appear to come from reputable sources. These attacks can take many forms,

including email, phone calls, and website impersonation, all with the goal of tricking victims into revealing sensitive data. Spoofing attacks come in various forms, like manipulating IP addresses, caller IDs, email addresses, websites, ARP, and DNS servers, each posing different risks to users and businesses.

Statistics on the rise of cyber threats globally and in the U.S. California

Globally

While there has been improvement in cyberspaces compare to the past couple of years, the development of more cyber threats and attacks remains a concern and seems to be rising along with the improvements being made. Globally, hackers and attackers have increasingly attacked bigger companies, brands, and operations, underlying the efforts their putting towards these cyber activities. In the past 12 months, according to the Controllership poll, 34.5% financial and accounting organizations have been receiving cyber threats, in that 34.5%, 22% have received at least one threat, the others have received more than one. 48.8% states that their organizations' confidential data have been targeted. The remaining 20.3% states that they have been working to protect their organization with their cybersecurity team, which seems to be effective when it comes to protecting confidential information in the company. Although there have been some advancements in cyberspace, the growing number of cyber threats that target large corporations worldwide continues to be a serious worry, underscoring the continuous efforts made by cybersecurity teams to protect sensitive data.

Cyber Threats in U.S. California

California

California being a large state with numerous technology and non-technology organizations, it has become a prime target for multiple and various attacks. California is the most targeted state for ransomware attacks, according to a report by cybersecurity company Abnormal Security titled "California Most Targeted State for Ransomware Attacks". According to the data that has been collected, 260 of the roughly 4,200 ransomware victims between 2020 and 2021 were in California. Hackers using ransomware lock victims' computers and demand cryptocurrency payments; such attacks usually begin with phishing emails. Huge amount of dollars is now typical ransom request. Organizations like Barlow Respiratory Hospital have been victims of cyberattacks despite the strong cybersecurity protocols, highlighting the persistent threat.

A significant hack that impacted colleges across the country also targeted Stanford and UC. The assault revealed personal data by taking advantage of a vulnerability in Accellion, a file transfer service, which prompted investigations. There were about 300 organizations impacted, including businesses and government organizations.

Impact of Cyber Threats on the state of California

Economic Impact/ Social Impact

The financial stability of the state as well as businesses and individuals are all negatively impacted by cyber threats in California. Annual damages from these risks amount to billions of dollars, according to the California Cybersecurity Integration Center (Cal-

CSIC). Not only do ransomware attacks, data breaches, and identity theft directly cost businesses millions, but they negatively impact customer trust, which discourages investment and spending. California's economy is further strained by the costs associated with recovery efforts and cybersecurity measures. To tackle these threats and prevent further economic disruptions, strong cybersecurity laws, investments in digital infrastructure, and collaboration between the public and private sectors will be required.

In the social aspect California, cyber threats have a significant social impact on individuals, businesses, and governmental organizations. The California Department of Justice claims that these dangers have contributed to financial fraud, identity theft, privacy violations, and trust in online transactions.

Political Impact

In California, cyber threats pose political risk to the state's democratic processes and the government. The California Secretary of State's office has recorded cases of interference in elections and attempts to undermine voter confidence by cyberattacks on electoral systems. Such acts endanger the integrity of elections while also destroying public trust in the democratic process. In addition, cyber threats sent or made towards government institutions and officials undermine their ability to serve the public effectively, causing disruptions in service delivery and policymaking. This means that keeping California safe from cyber-attacks and threats has become very important in political aspect. Lawmakers are

working hard to make strong rules to protect against these threats and keep our democratic systems protected or secure.

Vulnerabilities in California

In situations and instances involving threats, a vulnerability represents a weakness within a computer system that enables hackers to gain entry and exploit it for their personal purposes. From personal data theft to disrupting critical infrastructure, California faces a range of cyber threats due to these vulnerabilities. Outdated systems and software are a major problem. Like leaving your front door unsecured, using outdated software makes you a prime target for online thieves. Hackers prefer to exploit holes in these outdated systems so they can access undetected. Another vulnerability is human error in California. One wrong click on a suspicious link or a weak password can give cyber attackers a golden ticket into our systems. It's like leaving the keys in the ignition and the engine running; it invites trouble. Then there's the growing trend of remote work in this state. While it’s great for flexibility, it also opens new avenues for cyber threats. Employees who work from home may unintentionally expose important data to unwanted parties if strong security measures aren't in place. California is very advanced in technology, including innovative devices such as smart thermostats and connected cars, which have become common. However, most of these Internet of Things (IoT) devices lack basic security features. This vulnerability makes it possible for hackers to get into individuals' homes and operate these gadgets for malicious purposes.

Measures: Action & Reflection

California is improving its cyber defenses through the introduction of several prevent ative steps to protect its cyberspace. The California Cybersecurity Integration Center (Cal-CSIC) are proposing security measures and different type of defensive measures to help the state's cyberspace. Cal-CSIC has taken the lead on several important projects, including providing guidance to telecommuters. With the rise of remote work, the center recognizes the increased risks associated with telecommuting. As a result, they have put out policies and procedures that have successfully reducing these risks. Cal-CSIC's goal is to improve cybersecurity in California by educating teleworkers or remote workers on how to protect their remote work environments. Legislation was also passed in California to improve cybersecurity in many areas. The California Consumer Privacy Act (CCPA), for instance, imposes strict rules on companies to protect individuals' personal data and quickly alert customers in the event of a data breach. Similarly, the California Internet of Things (IoT) Security Law sets rules for connected devices sold in the state to stop cyber criminals from exploiting IoT weaknesses. Moreover, the state focuses on teaching people about cybersecurity and training them to handle new cyber threats. By spreading awareness and giving tailored training to teleworkers and others, California wants to give everyone the tools they need to stay safe online.

Future Outlook

Looking toward California's cybersecurity future, the state needs to grapple with the fact that cyber threats affect every aspect of society, how organizations operate, politics, economics, and social interactions. For organizations, the future of cybersecurity is looking at the interventions used to prevent future attacks. That is, businesses will have to continue putting up new protective barriers and technologies, like leveraging artificial intelligence and machine learning to detect and pre protectively respond to cyber-attacks as they happen. There will also be more of an emphasis on training and raising awareness for employees to identify and mitigate risks. As the cyberspace, businesses and institutions will have to focus more time and resources on cybersecurity in the planning and strategy stages.

As California looks to the future of cybersecurity, the state must consider how cyberth reats impact all areas of the society. Adding to the complexity, the regulatory environment, both at state and federal levels, will significantly influence California's cybersecurity. Adherence to policies and laws such as the California Consumer Privacy Act (CCPA) and the California Internet of Things (IoT) Security Law requires enterprises to strengthen their cybersecurity posture and prioritize protecting sensitive data.

On a more positive note, California is actively investing in cybersecurity infrastructure, encouraging workforce development, and developing public-private partnerships to strengthen its cyber defenses. Organizations like the California Cybersecurity Integration Center (Cal-CSIC) demonstrate the state's proactive approach to detecting and responding to threats.

In conclusion, cyber risks constitute a huge challenge to California, influencing the economy, society, and politics. The state suffers several cyber threats, including malware, phishing, and DDoS attacks, which are on the rise both globally and in the United States. California is particularly vulnerable because of its modern technological infrastructure and large use of Internet-connected devices. These cyber threats cause financial losses, damage to infrastructure, and compromise sensitive data. California's vulnerabilities, such as outdated systems and human error, increase the problem. However, the state is taking steps to improve cybersecurity by passing legislation and launching projects focused at improving data security and tackling IoT vulnerabilities. Moving forward, California must continue to invest in technological innovations, personnel training, and public-private partnerships to successfully minimize cyber threats. By remaining proactive and collaborative, the state can strengthen its cyber defenses and protect the safety of its citizens and organizations in this new age of technology.

References

Brooks, Chuck. “Cybersecurity Trends & Statistics for 2023; What You Need to Know.” *Forbes*, Forbes Magazine, 20 Feb. 2024, www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=1746eeb419db.

California, State of. “California Cyber Security Integration Center Offers Guidance for Teleworkers.” *California Cyber Security Integration Center Offers Guidance for Teleworkers | Cal OES News*, news.caloes.ca.gov/california-cyber-security-integration-center-offers-guidance-for-teleworkers/. Accessed 21 Apr. 2024.

California, State of. “Home.” *California Governor’s Office of Emergency Services*, www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/. Accessed 21 Apr. 2024.

KnowBe4. “What Is Phishing?” *Phishing*, www.phishing.org/what-is-phishing. Accessed 21 Apr. 2024.

“Report: California Most Targeted State for Ransomware Attacks.” *CBS News*, CBS Interactive, 28 Jan. 2022, www.cbsnews.com/losangeles/news/report-california-most-targeted-state-for-ransomware-attacks/.

“Resources for Victims.” *State of California - Department of Justice - Office of the Attorney General*, 11 May 2022, www.oag.ca.gov/cyberexploitation/victims.

Roy, Raj, et al. “What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples - Spiceworks.” *Spiceworks Inc*, 23 Aug. 2021, www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat/.

“Stanford, University of California Targeted in Widespread Ransomware Cyber Attack.” *CBS News*, CBS Interactive, 3 Apr. 2021, www.cbsnews.com/sanfrancisco/news/stanford-university-of-california-targeted-in-widespread-ransomware-cyber-attack/.

“What Is a Spoofing Attack? Detection & Prevention.” *Rapid7*, www.rapid7.com/fundamentals/spoofing-attacks/. Accessed 21 Apr. 2024.