CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

SUMMARY

Nationwide, a cyber-attack occurs at least every 39 seconds. Globally, the cost of cyber-attacks is expected to be \$6 trillion by 2021[1]. The 2019-20 Santa Barbara County Grand Jury through its research learned the County of Santa Barbara, the eight incorporated cities, and the special districts within the County, as a whole, are woefully ill-prepared for a cyber-attack. Such an attack could cripple their services and data systems. The cost to repair and recover these systems could be millions of dollars![2] Cyber security attacks include corruption or theft of data, denial of service, or complete destruction of critical data. Also, attacks could include subverting critical operations, such as water systems, electrical grids, and communication systems, and thus threaten public safety.

Cyber-attacks are more widespread and dangerous than is generally recognized, even by people who should know. The attacks are certain to get worse. There is a never-ending evolutionary race between attack and defense. In this digital world, local government entities, even small ones, are not immune and their risks will grow as automated attack methods increase.

INTRODUCTION

According to a recent survey of national business leaders, cyber security risks are the top concern among businesses of all sizes, ahead of medical cost inflation, employee benefit costs, the ability to attract and retain talent, and legal liability.[3] Fewer than half of all Chief Information Security Officers and senior executives are confident their organizations are fully prepared to deal with cyber-attacks, according to a study conducted by a well-known cyber security consultancy.[4]

Whether the cyber-attack is motivated by money, revenge, mischief or geo-politics, the costs to respond and recover can be astronomical. These attacks can be in the form of:

- **Data theft**, the unauthorized taking or interception of computer-based information.

- **Ransomware**, a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

---

[1] Herjavec Group: The 2019 Official Annual Cybercrime Report. https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report (Last visited 02/03/2020)

[2] "Texas Ransomware attack to cost \$12 million and more", *Cybersecurity Insiders,* https://www.cybersecurity-insiders.com/texas-ransomware-attack-to-cost-12-million-and-more/ (Last visited 02/03/2020)

[3] "2018 Travelers Risk Index: Cyber [Infographic]", *Travelers*, 2018 https://www.travelers.com/resources/risk-index/2018-cyber-infographic (Last visited 03/12/2020)

[4] "Cyber Tops All Other Risk Concerns for Businesses of All Sizes", *Insurance Journal*, October 1, 2019 https://www.insurancejournal.com/news/national/2019/10/01/541645.htm (Last visited 02/03/2020)

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

- **Sabotage**, deliberate attacks intended to disable or modify computers or networks for the purpose of disrupting operations or transactions, accessing or destroying files or otherwise compromising an organization.

The Jury reviewed many news reports of cyber-attacks on public entities, a few of which are summarized below:

A ransomware attack in March 2018 paralyzed Atlanta's 424 software programs, of which 30% were mission critical. Atlanta refused to pay the ransom of $51,000 and it ultimately cost the city $21 million to recover their systems.[5]

In May 2019, Baltimore refused to pay a $76,000 ransom demand resulting in weeks of downtime and system upgrade costs of $18 million. Subsequently, the city purchased insurance policies totaling $20 million, with an annual premium of $835,103.[6]

As recently as July 2019, Los Angeles city computers were breached, resulting in the theft of the personal information of approximately 20,000 applicants to the police department. The information stolen did not directly impact the city, but could be used to compromise the privacy of the individuals, and allow the criminals to open credit cards, take out loans, intercept tax refunds, and otherwise disrupt an individual's credit.[7]

In August 2019, $4.2 million was stolen from the Oklahoma Law Enforcement Retirement System after an employee's account was compromised.[8]

In October 2019, it was reported there were more than 140 ransomware demands in the last 10 months across the United States. These attacks were made on county, city, or state government systems, including health care systems and police departments.[9]

While sabotage of governmental computer systems and networks has not yet been reported as widespread, there have been instances which demonstrate it is a valid concern. In 2013, a New York

---

[5] Lee Matthews, "City Of Atlanta Computers Hit By Ransomware Attack", *Forbes*, March 23, 2018 https://www.forbes.com/sites/leemathews/2018/03/23/city-of-atlanta-computers-hit-by-ransomware-attack/#3a8316812ee4 (Last visited 02/03/2020)

[6] Sarah Cole, "Baltimore Doubles Up on Cyber-Insurance Following Ransomware Attack", *Infosecurity Group*, October 18,2019 https://www.infosecurity-magazine.com/news/baltimore-buys-cyber-insurance/ (Last visited 02/03/2020)

[7] Cindy Chang, David Zahniser, "City computers breached, data potentially stolen from 20,000 LAPD applicants,' *Los Angeles Times*, July 29,2019 https://www.latimes.com/california/story/2019-07-29/lapd-applicants-data-breach (Last visited 02/03/2020)

[8] Nolan Clay, "Hackers get $4.2 million from Oklahoma pension fund for retired troopers, state agents", *The Oklahoman*, September 6, 2019 http://oklahoman.com/article/5640503/hackers-get-42-million-from-pension-fund-for-retired-troopers-state-agents (Last visited 02/03/2020)

[9] Allen Kim, " In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks", *CNN.com,* October 8, 2019 https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html (Last visited 02/03/2020)

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

dam's control system was hacked by a foreign group.[10] In January 2020, the Federal Depository Library Program's website was hijacked, and a pro-Iranian message was displayed.[11]

In January 2020 in Santa Barbara County, the Carpinteria Unified School District was attacked by ransomware, temporarily shutting down the district's networked computers and creating $90,000 in damage.[12]

Cyber security is a critical element of today's world of computerized life. Types of attacks that can occur include:

- *Phishing* is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

- *Harvesting employee credentials, also known as password harvesting,* takes many forms, including phishing, and is used to steal user credentials. Credential-harvesting attacks often start with targeted phishing emails that request the victim to click on a link and log into their own account to change password or payment information. The link then directs the user to a spoofed[13] site, allowing the hacker to harvest the valid credentials entered by the victim, and then use those to log into the victim's actual account.

- *Backdoor* is a method of bypassing authentication in a piece of software or a computer system allowing access without being detected.

- *Social engineering* is manipulating people to give up confidential information. The type of information sought includes passwords, bank information and other personal information. It can also help someone gain access to your computer to secretly install malicious software, allowing them access to and control of your confidential information.

- *Programming bug* is a programming error in the computer code that results in faulty results or information. It can also allow for unwanted access to a computer system or network.

- *Outdated software* is software that is no longer fully supported by the vendor which can make it easier to attack through known flaws and weaknesses in the system.

---

[10] Joseph Burger, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case", *The New York Times*, March 25, 2016 https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case html (Last visited 02/03/2020)

[11] Mihir Zaveri, "Government Website Is Hacked With Pro-Iran Messages", *The New York Times*, January 6, 2020 https://www.nytimes.com/2020/01/06/us/iran-hack-federal-depository-library.html (Last visited 02/03/2020)

[12] Debra Herrick, "CUSD Hit By Malware…", *Coastal View News* (January 23, 2020)

[13] Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. *https://www.forcepoint.com/cyber-edu/spoofing* (Last visited 02/17/2020)

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

- *Unpatched software* is software that has not been updated to the latest version provided by the vendor. Similar to outdated software, it can be easier to attack.

- *System misconfiguration* is when settings within a computer program are not configured properly and could allow unauthorized access or unintended consequences.

- *Inside attack* is an attack by someone with authorized access to a computer system or network that uses the access in ways not approved or granted by the organization. This can sometimes occur when a terminated employee's system access has not been revoked on a timely basis.

- *Physical attack* involves gaining access to computer systems and networks through physical means. This includes unauthorized access to facilities and buildings but can also include accessing the systems and networks by using an unattended computer terminal.

Every public entity within Santa Barbara County needs to be familiar with these dangers and threats and the steps that need to be taken to prevent them.

METHODOLOGY

The Grand Jury interviewed two well-known experts on cybersecurity, a Certified Information Systems Security Professional and a highly credentialed Independent Information Security Analyst. The Jury attended an all-day Cybersecurity Summit at UC Santa Barbara, which included seminars and interaction with speakers and attendees. The Jury also reviewed a large number of studies, news reports and professional articles related to cyber security.

The Jury interviewed individuals who have extensive experience in cyber security. Their experiences include:

- Oversight of information technology security for private enterprise and government organizations
- Presidency of information security management service organizations
- Service on cyber security task forces
- Work in national information security

To get an overview of the general status of cyber security awareness within the County, the Grand Jury sent surveys to many governmental entities within the County, including the incorporated cities, special districts and the County itself. The surveys were emailed to administrators and Information Technology (IT) department heads. The surveys covered a variety of cyber security issues, including the nature of their systems and how they are administered, whether there is a written cyber security plan and if it has been tested, whether cyber security audits are performed and when the last audit was, and whether they have cyber insurance and what kind.

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

OBSERVATIONS

The responses to the Grand Jury's survey showed most entities were deficient in one or more critical areas. Many of those surveyed reported that they had no cyber security plan, had never performed a security audit and carried no cyber insurance.

Clearly, many public entities within Santa Barbara County are not fully prepared to withstand a cyber-attack.

Important Concepts and Best Practices:

As a result of its investigation, the Grand Jury found the following important concepts and best practices should be implemented as soon as possible to lower an organization's risks from cyber threats and damage:

- *Identify someone to be in charge.* Organizations should appoint a designated individual with the proper expertise who is granted authority to be accountable and responsible for all cyber security, including managed service providers.[14]

- *Identify the nature of the organization's data and the electronic systems employed and understand the security risks.* Organizations should understand what type of data they maintain and use in the execution of their mission and the electronic systems employed that do, or could, allow access to the data. How is the data handled and protected to prevent unauthorized use? Who has access to that data and under what circumstances? What are risks related to unauthorized access or, in the worst case, destruction of the organization's data?

- *Establish a written cyber security plan.* A cyber security plan adds a layer of protection to an organization's important resources. Protecting important data and related systems is important, not only for the organization, but also its customers. Cybercrime is escalating and having a strong defense and recovery plan helps protect the organization's reputation. A well written plan should not only detail the preventative steps the organization needs to take to prevent an attack, but also provide a recovery plan in case the data is attacked, corrupted or otherwise compromised.

- *Protect data from internal and external threats.* Data can be attacked or compromised from many sources, whether intentional or by accident. Protecting an organization's data and systems from an external threat and intentional attack is not enough—they also must be protected from unauthorized internal access, accidental corruption or destruction. An organization's plan needs to identify and

---

[14] Edward Gately, "ESET: MSPs Not Proactive Enough with Cybersecurity", *ChannelFutures.com*, February 7, 2020 https://www.channelfutures.com/channel-research/eset-msps-not-proactive-enough-with-cybersecurity. (Last visited 02/10/2020)

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

address all possible threats and should require periodic changing of all passwords and making sure sensitive systems are contained in a secure environment with controlled access.

- ***Have strong firewalls, appropriate authorization and access controls, and effective antivirus software.*** Strong firewalls prevent unauthorized outside access to an organization's systems and data. If an attacker cannot get into the system, it is harder for them to disrupt operations or damage or steal data. Having an appropriate authorization and access control system helps, among other things, assure that employees and authorized contractors can access only the systems and data they require to properly execute their duties and helps prevent unauthorized activities, theft, corruption or destruction of data. Antivirus software helps prevent software viruses, worms, "Trojan Horses," spyware or malware from being downloaded to an organization's electronic systems, as well as increasing protection from phishing attacks.

- ***Install and update software regularly.*** Using the correct software and keeping it updated frequently is a strong step to help prevent attacks. Software providers are continually updating and improving their products to not only make it more effective but to address flaws that are discovered that could be used to attack an organization's systems or data. Old and out-of-date software is much more vulnerable than current software. Software should not only be updated on internal equipment but also on all portable devices that have access to the organization's systems.

- ***Maintain cyber security awareness and training for all employees.*** A system is only as strong as the people who are using it. While there are many ways to attack a system electronically, one of the easiest ways to get access to a system is to trick someone to open the door for you. This "social engineering" is cheap, effective and quicker than trying to break into a system through other means. Employees and contractors with access to the system should be made aware of the dangers of social engineering and phishing scams, and be trained how to prevent access through these means. This awareness and training should focus not only on electronic devices provided by the organization but also personal and portable electronic devices that have access to the organization's system via Wi-Fi, email or the internet.

- ***Create a recovery plan.*** While planning and prevention is a vital component to strong cyber security, the reality is that things can go wrong, attackers can succeed, and things break. Therefore, it is very important that an organization have a detailed and documented recovery plan. This plan, among other things, should include periodic backups, and safe offsite storage of backup data and system software.

- ***Regularly update and test the plan.*** Just like practice fire drills are an important component of assuring the safety of employees, practicing the steps of an organization's cyber security plan, especially the recovery components of the plan, is vitally important. Practice runs not only help to confirm if the plan works and what improvements could be made, they also prepare the organization for a fast response in the case of an actual attack.

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

- ***Consider working with other organizations to improve cyber security practices cost effectively.*** Working as a consortium provides an approach allowing even those with smaller budgets to participate and contribute to a successful security program.[15]

CONCLUSIONS

The 2019-20 Santa Barbara County Grand Jury determined that cyber-attacks and related threats are an ongoing reality and that all public entities within Santa Barbara County need to take prompt and aggressive steps to prevent significant disruption from these attacks. When cyber-attacks are successful, the costs to respond and recover can be in the millions of dollars. While some local public entities are taking steps to protect themselves from these risks, many are not adequately prepared.

FINDINGS AND RECOMMENDATIONS

Finding 1
Ensuring critical cyber security tasks and activities are properly executed on a timely basis requires a designated individual to be accountable and responsible.

Recommendation 1
That each public entity within Santa Barbara County designate an individual to be accountable and responsible to oversee cyber security.

Finding 2
Most public entities within Santa Barbara County have an inadequate understanding of what communication and electronic systems they use and what data they maintain, and do not fully understand the risks, security issues and costs associated with the destruction of systems or loss of data.

Recommendation 2
That each public entity within Santa Barbara County complete a full inventory of their data, electronic and communication systems and determine the related security risks.

Finding 3
Some public entities within Santa Barbara County do not have a written cyber security plan.

Recommendation 3
That each public entity within Santa Barbara County establish a written cyber security plan.

---

[15] Wany Zhao and Gregory White, "A collaborative information sharing framework for community cyber security," published in Homeland Security (HST), 2012 IEEE Conference on Technologies for Homeland Security (HST), November 13-15, 2012

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

Finding 4
Nationally, cyber-attacks on governmental organizations have been successful for many years and are occurring with more frequency and sophistication.

Recommendation 4
That each public entity within Santa Barbara County take substantial steps to protect data from internal and external attacks or threats.

Finding 5
Cyber-attackers use a number of methods to install malicious software on systems including access through backdoors, staff or employee carelessness, and known bugs in software.

Recommendation 5a
That each public entity within Santa Barbara County install and maintain current antivirus software to detect malware and other threats.

Recommendation 5b
That each public entity within Santa Barbara County install and update all operating software regularly.

Recommendation 5c
That each public entity within Santa Barbara County periodically train employees and then test their cyber security awareness.

Recommendation 5d
That each public entity within Santa Barbara County periodically ensure electronic system-related contractors have been trained for cyber security awareness.

Finding 6
If data is lost or compromised for any reason, including cyber-attack, mechanical failure or error, the most cost effective and expedient way to recover is to have current data backups and a plan to reinstall it.

Recommendation 6a
That each public entity within Santa Barbara County create and implement a full backup and recovery plan.

Recommendation 6b
That each public entity within Santa Barbara County regularly update and test their backup and recovery plan.

Finding 7
Some public entities within Santa Barbara County do not have any, or adequate, cyber insurance.

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

Recommendation 7
That each public entity within Santa Barbara County secure adequate cyber insurance.

Finding 8
A cost-effective method to address cyber risks and concerns is to form an information sharing and learning consortium.

Recommendation 8
That each public entity within Santa Barbara County that is unable to allocate adequate funds for cyber security develop a cybersecurity working group to establish best practices and share costs for education, expertise, and insurance.

REQUEST FOR RESPONSE

Pursuant to *California Penal Code Sections 933 and 933.05*, the Santa Barbara County Grand Jury requests each entity or individual named below to respond to the enumerated findings and recommendations with the specified statutory time limit:

Responses to Findings shall be either:

- Agree
- Disagree wholly
- Disagree partially with an explanation

Responses to Recommendations shall be one of the following:

- Has been implemented, with brief summary of implementation actions taken
- Will be implemented, with an implementation schedule
- Requires further analysis, with analysis completion date of no more than six months after the issuance of the report
- Will not be implemented, with an explanation of why

Santa Barbara County Board of Supervisors — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Buellton — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

CYBER-ATTACKS THREATEN SANTA BARBARA COUNTY

City of Carpinteria — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Goleta — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Guadalupe — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Lompoc — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Santa Barbara — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Santa Maria — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8

City of Solvang — 90 Days

Findings 1, 2, 3, 4, 5, 6, 7, and 8
Recommendation 1, 2, 3, 4, 5a, 5b, 5c, 5d, 6a, 6b, 7, 8