Minnesota County Cybersecurity Survey Report

An examination of counties' cybersecurity maturity

Presented by
Mireille Ghassan
AMC Summer Intern
In an age where technology is changing and expanding at an accelerated rate, now more than ever local government leaders must place an emphasis on disaster resilience and preparedness. In today's world, it is not an option to place safeguards in place to protect against cyberattacks. It is a must.

According to the cybersecurity firm Emsisoft, in 2019, the United States experienced “…an unprecedented and unrelenting barrage of ransomware attacks that impacted at least 966 government agencies, educational establishments, and healthcare providers at a potential cost in excess of $7.5 billion.”(1) Prominently included among organizations hit by ransomware attacks were 113 local and state governments and agencies.

Objectives

- Better understand the cybersecurity environment across all Minnesota counties.
- Determine various factors that lead to strong cybersecurity safeguards.
  - Assess counties that have had a cyberattack in the last 5 years.
- Determine the percentage of counties that believe they lack the resources needed to establish strong cybersecurity safeguards.
  - Compare and contrast the similarities and differences amongst the various counties' policies and procedures.
- Understand what makes for strong cybersecurity safeguards
  - Showcase the benefit of investing in cybersecurity safeguards versus what it would cost if an attack were to happen.
Summary of Findings

After receiving feedback from 51 of the 87 county CIOs, IT managers and directors in Minnesota, it is clear that the cybersecurity is growing rapidly and evolving faster than we can comprehend. Most if not all counties at least have some sort of security but by no means a cybersecurity system to rely on long-term in event of an attack. Throughout the state there are many vulnerabilities within the cybersecurity environment. This is due to the fact that cybersecurity is an ever changing field and it becomes difficult to continuously stay up to date with all the new software and security system updates. This survey revealed that counties, especially those that are less populated, lack the necessary resources to build a safe and secure network, along with a cybersecurity response plan. The resources counties lack include staff, funding, training, and education.
Survey Analysis

Q. Has your organization, in the past 5 years, experienced any of the following cyber-incidents? Please select all that apply.

Answered: 47  
Skipped: 4

The first question of the survey was to assess how many counties have experienced some sort of cyber-incident, and then to further distinguish which form of attack took place. In some cases, there have been one or two different types of attacks at the same time. Forty-seven counties have reported having a cyber incident, making that more than 50% of counties. Phishing without a doubt is the most common reason for a breach of any sort. It is important to note that local governments, public administration, agencies, educational organizations, and hospitals are considered soft targets, meaning they are easily accessible due to their strict budgets and lack of security.
Q. Have you quantified and assessed the potential financial impact of an interruption caused by a cyber event?

Answered: 51  
Skiped: 0

Well over half of the respondents, 36 counties, have not assessed the impact of a cyber event on any level. Cybersecurity risk and impact assessments are crucial to the financial stability of counties as it not only helps to educate people within the organization on threats the organization may face, but also how those threats can potentially impact roles within the organization itself. According to Comparitech, in 2020, 79 individual ransomware attacks were carried out against US government organizations, which impacted 71 million people and costed an estimated $18.88 billion in downtime and recovery costs (2). The average ransom demanded by hackers in 2020 from government related organizations was $570,857, with over $1.75 million actually paid.
Survey Analysis

Q. Do you have a data security incident response plan?

Answered: 51  
Skipped: 0

According to The National Institute of Standards and Technology, an incident response plan is “a predetermined set of instructions or procedures to detect, respond to and limit consequences of a malicious cyberattacks against an organization’s information system”. Incident response plans are put into place because of cybersecurity insurance companies, which a majority of state and local governments have, will often require that they be the first contact in the event of an attack. Without an incident response plan, that reporting requirement could get missed, and agencies would then be in violation of their agreement with the insurance company (3). Not only should governments have a plan in place, but also take the time to practice it frequently to make sure everything is up-to-date and secure.
Q. Do you wish you had more resources to invest in cybersecurity?

Answered: 51  
Skipped: 0

IT professionals overwhelmingly agree that counties need to invest additional resources in to IT and cybersecurity. Not only should the priority be to maintain, improve and adapt their systems but to also protect their citizens information from being exploited or breached by bad actors. Cybersecurity is constantly and will continue to evolve as technology incessantly expands and upgrades. State and federal officials are recognizing a need for more cybersecurity investments, and are starting to make plans for future cybersecurity improvements, upgrades and investments. Counties should prepare for this investment opportunity, as now is a prime time to start strategically planning ahead and assess where improvement is needed.
When it comes to staffing full-time IT employees, the number varies quite drastically, and this makes sense as the smaller, less populated counties have less staff, and more densely populated counties require more staff. As you move from counties with a population of 50,000 - 100,000 to counties with a population of over 100,000 the average number of staff increases by 949.02%. Not only is this concerning for the smaller counties’ IT departments, but it also reveals the importance of investing in IT in smaller populated areas.
Glossary

**Brute force**: An attack method where an attacker uses a tool such as software to continuously “bang away” to gain access to a victim’s computer, network, or IT system.

**Authentication**: The process of verifying the identity of a user who is logging onto a computer system or verifying the origin of a transmitted message.

**Backup**: The process of transferring software and data to alternative media, such as tape, to be used to recover systems in the event of system malfunction or disaster.

**Critical Application**: An application that is so important that its malfunction, loss, or unavailability would have a significant impact on the continued operation of the County.

**Denial of Service (DoS)**: An attack that sends massive volumes of traffic to overwhelm an organization’s website or server.

**Distributed Denial of Service (DDoS)**: A type of DoS attack that uses multiple computers simultaneously to shut down a website or server to all users.

**Disaster Recovery Plan**: Documents steps that must be taken to recover electronic systems and processes in the event of a system malfunction or a disaster.

**Encryption**: A technique used to protect data by transforming the data from the original format to a difficult to interpret format.

**Firewall**: A method, device, or software that is used to implement security policies designed to keep a network secure from intruders.

**Hacker**: An unauthorized user who attempts to or gains access to an information system.

**IP Address**: A series of numbers that identifies any device on a network.

**Malware**: Malicious software installed that can encrypt data and files, block user access, exfiltrate data and files, etc.
Phishing: A form of social engineering in which cybercriminals “go fishing” for victims by sending emails, seemingly from trusted parties, with promises, opportunities, or threats to deceive victims.

Ransomware: Type of malware that encrypts sensitive data and files to then demand a ransom to unlock the encrypted information.

Smishing: A phishing cybersecurity attack carried out over mobile text messaging, also known as SMS phishing.

Spear phishing: Spear phishing is a more sophisticated form of phishing in which the cybercriminal uses just enough information to make the victim believe the email came from someone known to the victim or another trusted source.

Trojan horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Vishing: An electronic fraud tactic in which individuals are tricked over the phone into revealing critical financial or personal information to unauthorized entities.

Virus: A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Zero-day: An attacker’s identification of a weakness in a network or IT system, such as utilizing defects in outdated software versions.
Sources


