An Update on Cybersecurity for Local Governments in South Dakota:
The Top Findings from Project Boundary Fence

By: Arica Kulm, Ph.D., Director of Digital Forensics Services, DigForCE Lab, Dakota State University, & Dave Pfeifle, SDPAA Executive Director

For many years the cyber experts at Dakota State University (DSU) have been assisting local law enforcement agencies in South Dakota with cyber forensic services. More recently, DSU began "Project Boundary Fence" to provide free cybersecurity assessments including penetration testing, social engineering awareness, vulnerability assessments and more to all local governments in South Dakota. Their testing identifies risk factors and possible attack vectors for these local governments' IT systems, then recommends possible solutions. In July 2021, the South Dakota Public Assurance Alliance (SDPAA) announced to SDPAA Members that all local governments were eligible to participate for free in DSU's program. To date, almost 90 SDPAA Members and dozens of other local governments have enrolled in the program. On behalf of SDPAA Members and other local governments in South Dakota: Thank you, DSU!

Funding for this vital program has been provided through the South Dakota Attorney General's Office, Division of Consumer Protection. Much of this funding comes from the settlement funds the State of South Dakota received from various data breaches suffered by major companies which potentially impacted thousands of citizens in South Dakota. The services of this program are available while funding remains. If your public entity has not enrolled in this program, please immediately contact projectboundaryfence@dsu.edu regarding these services and please visit https://dsu.edu/boundary-fence/ for more information.

DSU utilizes its world-class cyber expertise to serve the local governments in South Dakota and has established a flagship program which provides a template for others across the nation. The confidentiality of DSU's findings for a local government's particular cyber vulnerabilities is fully protected when a local government enrolls in this program. This article will briefly share the common vulnerabilities identified from this testing and then some recommended solutions.

Overall, DSU's testing has confirmed the main attack vector for a cyberattack is through a local government's email. Approximately 90% of the cyber risk for a local government is estimated to emanate from email. South Dakota's local governments have over 13,000 employees, vendors, and others who are using their local governments' IT networks through a wide range of email systems. Any one of these "end users" could accidentally click on a phishing email or the like to expose the entire system to a ransomware attack or other attack on the local government's IT system. A ransomware attack will infect a system and render it inoperable unless an exorbitant ransom is paid. The attack will also acquire and "freeze" more sensitive citizen data and then threaten to release it unless that ransom is paid. Cyberattacks on local governments have included a malicious reset of the amount of chemicals used at a local wastewater treatment plant in Florida. This cyberattack would have poisoned or killed thousands of people absent a last-minute human intervention.

The cyber forensic assessments by DSU and other experts prove the "human firewall" is the most crucial aspect of cybersecurity. End user awareness and vigilance remain the best means of preventing a cyberattack. DSU, the SDPAA, the South Dakota Municipal League, the South Dakota Association of County Commissioners, the South Dakota Association of County Officials, among others have been offering many cyber training opportunities on-line and in-person for all local governments in South Dakota. Please ensure you and your team partake in these training opportunities to help protect your public entity and the citizens you serve from such an attack.

The list below represents the top findings from the penetration testing by DSU over the past year:

1. *Passwords, Passwords, Passwords*

Weak passwords and improperly stored passwords are the top finding that DSU's testers are identifying when performing their assessments. From default passwords being used, to very simple passwords, to files stored on the system labeled "Passwords" containing logins to other areas of the network, these poor password hygiene habits can be harmful to a local government's system. A system is only as strong as its weakest link, so one weak password can make an entire system vulnerable. These password findings can be summarized in three main areas:

a. Weak Passwords:

A weak password is short, easy to guess, a system default, or otherwise easily detectable. The table below shows how quickly a shorter, less complex password can be compromised. All end users should use longer, more complex passwords. Use combinations of letters, numbers, uppercase, lowercase, and symbols. The longer the password the better – consider a pass phrase over a password (quaking unwieldy graceful unveiling playset).

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

b. *Password reuse:*

In 2021, there were over 6.7 billion pairs of unique user credentials found for sale on the dark web. (Vigliarolo, 2022) Using your work email/password on other sites makes both sites vulnerable if one is breached. Hackers buy these user credentials and use them to try to login to your system. They no longer need technical skills to try to hack into your system, they simply login as if they were you. Use unique passwords on each site you login to.

c. Password Storage:

Storing passwords on a file on your network – especially in an unencrypted file labeled "Passwords" – leaves your internal system very vulnerable. Even if external access is limited or highly secure, all it takes is one phishing email to get through, a hacker finds that file, and your entire network is then vulnerable.

Chrome, Safari, Edge, or other browsers are not secure places to store passwords. Each will ask you to store passwords; however, anyone who sits down at your computer has access to your passwords through the browser.

d. Password Strategies

It is hard to remember passwords for every different site or program – use a password manager. Some examples are listed below – Project Boundary Fence does not endorse one specifically, other options are available, use what fits your situation and needs. Many have free trials that do not expire or have minimal fees.

1Password - https://1password.com

LastPass - https://www.lastpass.com

KeePass – https://keepass.info

Dashlane - https://www.dashlane.com

e. Other Password Mitigation strategies:

Test your password strength:

https://www.security.org/how-secure-is-my-password/

Has your email or phone number been in a data breach? - https://haveibeenpwned.com
If your email address is found to have been in a data breach (this is not unusual), change your password on the site that was breached as well as any additional sites that utilize that same username/password combination.

2. Other Project Boundary Fence Significant Findings:

a. *Lack of endpoint protection (protection on each computer on the network).*

Each workstation should have, at minimum, anti-virus protection installed and current. Windows Defender comes installed with Windows 10 and Windows 11 and is a good basic option. For added security, add another layer of endpoint protection.

b. *Default configuration on devices installed on the network*.

Workstations, printers, WiFi, cameras – these, and other devices, should be configured to your system when they are installed and not just taken out of the box and plugged in. They often come with default credentials (login and passwords) that should be changed. Default credentials can be found in online user manuals that hackers can look up and use to compromise your network. Be sure to configure these devices to your individual network when they are installed.

These top findings represent cyber risks which can be remediated or prevented through good "cyber hygiene" practices. The solutions are relatively inexpensive and require a minimal effort to implement.