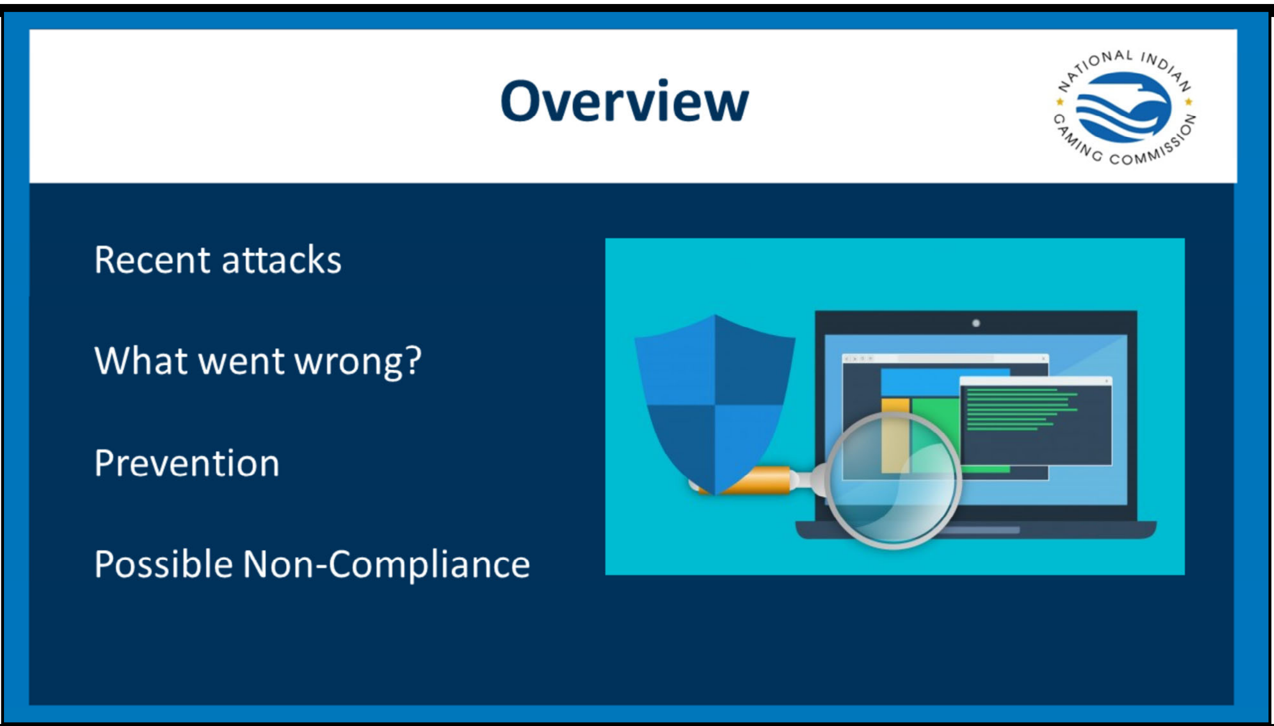
Critical Events Response & Preparedness - Cyber attacks

Division of Technology

Key Points:

PARTICIPANT QUESTION CHALLENGE
The time allotted for this virtual training will allow each of you to ask questions. I challenge each of you to ask a question! Your participation will make this training a success today!

My Notes:



Overview

Recent attacks

What went wrong?

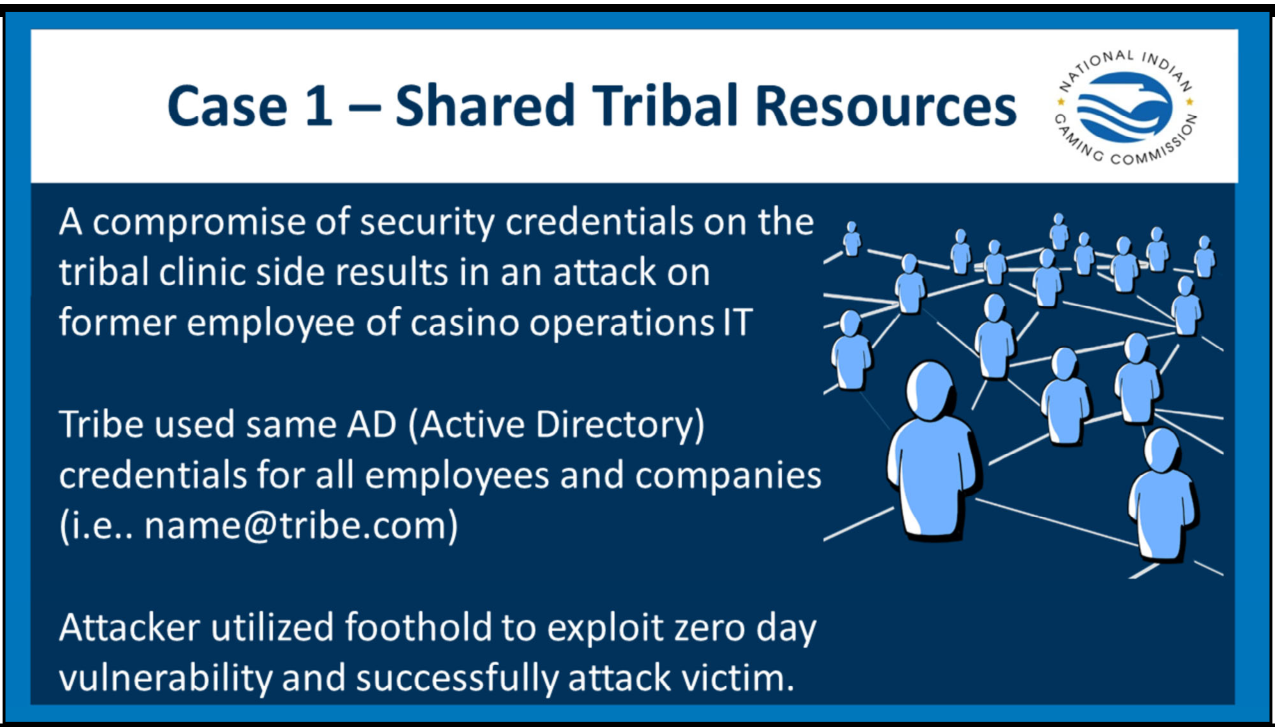
Prevention

Possible Non-Compliance

Key Points:

Rather than discuss specific types of trending attacks and vulnerabilities, in this course we aim to take a different approach. We will be looking at specific data/events/timelines of successful cyber attacks within Indian Country in recent years, and then by reviewing what happened in those attacks we will discuss lessons learned, ways to reduce the chance of a similar attack, and uncover possible lapses in compliance.

My Notes:



Case 1 – Shared Tribal Resources

A compromise of security credentials on the tribal clinic side results in an attack on former employee of casino operations IT

Tribe used same AD (Active Directory) credentials for all employees and companies (i.e.. name@tribe.com)

Attacker utilized foothold to exploit zero day vulnerability and successfully attack victim.

Key Points:

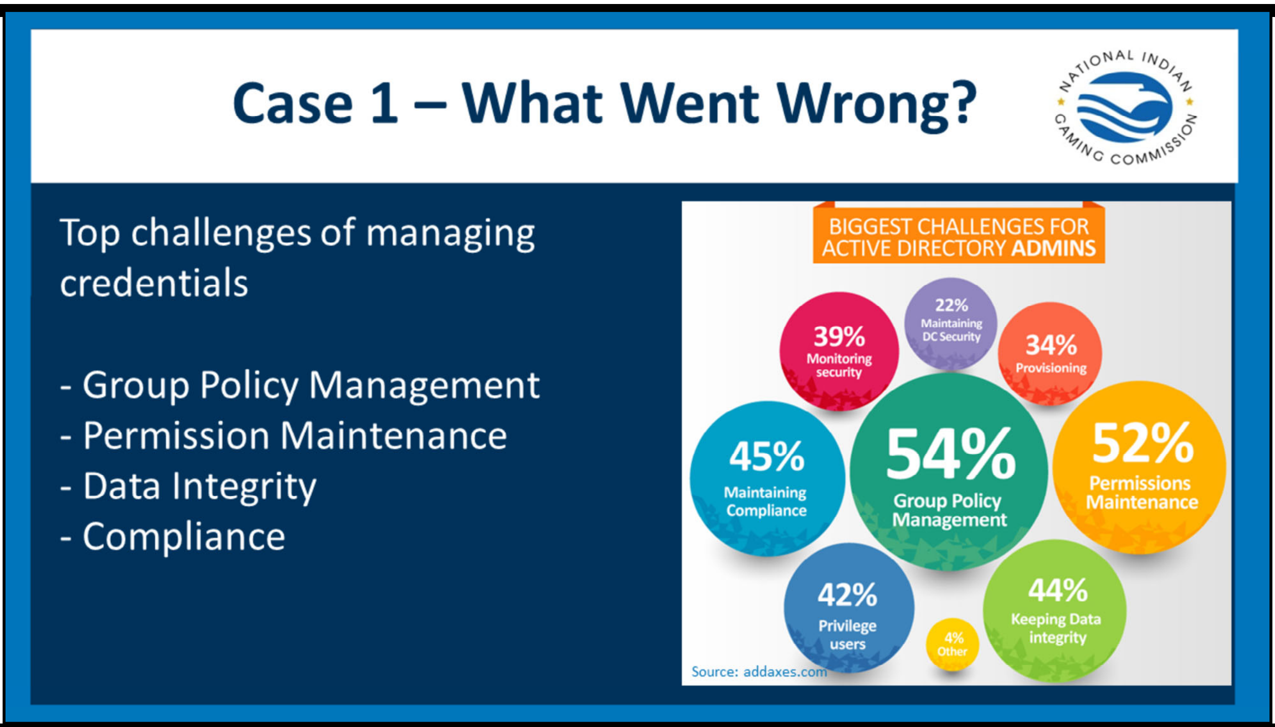
Attackers are able to obtain user credentials by attacking a tribal clinic. Employee had active credentials on the casino side. From this toe-hold they were able to exploit a zero-day vulnerability

Key Terms:

AD (Active Directory) – is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. While It is perhaps most commonly used to authenticate and authorize users and computers within a Windows domain type network, Active Directory has become an umbrella title for a broad range of directory-based identity-related services.

Zero-Day - a computer-software vulnerability either unknown to those who should be interested in its mitigation (including the vendor of the target software) or known and without a patch to correct it. Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers or a network.

My Notes:



Case 1 – What Went Wrong?

Top challenges of managing credentials

- Group Policy Management
- Permission Maintenance
- Data Integrity
- Compliance

Source: addaxes.com

Key Points:

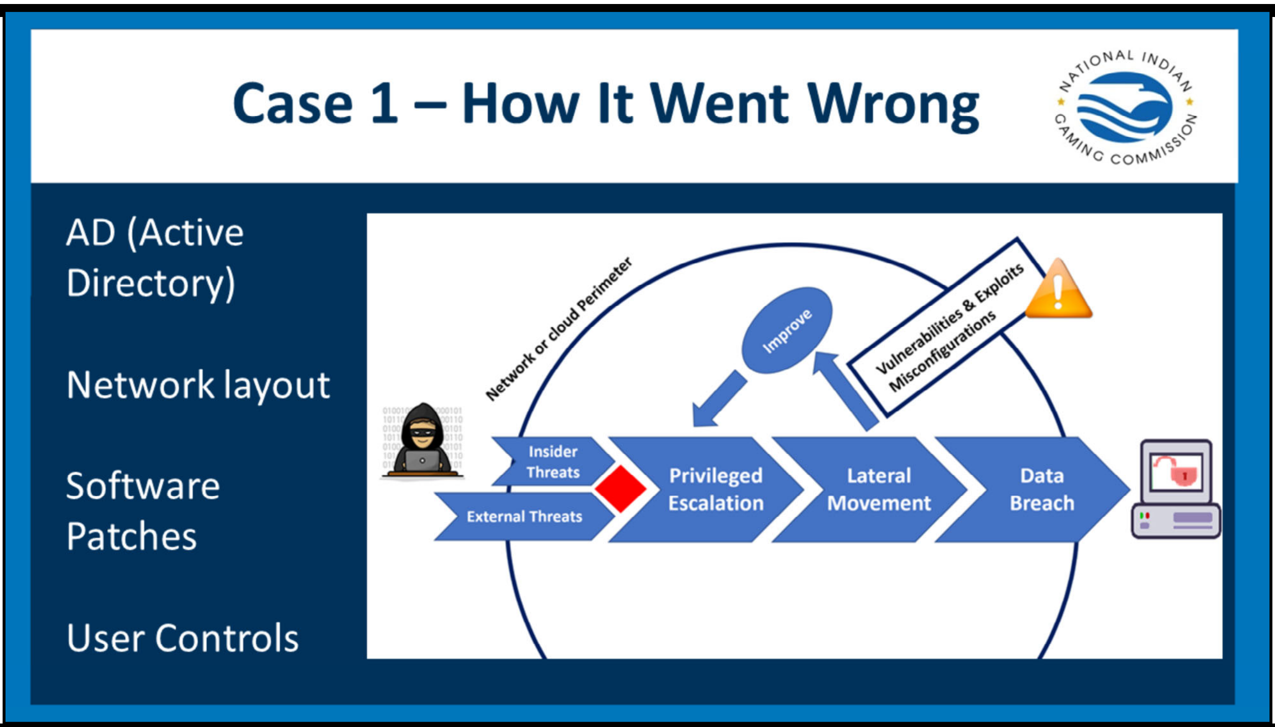
One aspect of the attack was the credentialing and user managing system, in this case Active Directory. Why is that such a challenge? On the surface it seems like a positive cost saving time saver to have a similar login for all aspect of the tribe.

But what are some of the areas where things can go wrong.

Common answers in surveys about AD management challenges point to:

- Group Policy Management – think Logical Security Controls 543.20(e)
- Permission Maintenance – think User Controls 543.20(f)
- Data Integrity – think Installation and Modification 543.20(g) and Data Backups 543.20(j)
- Compliance – think Following the SICS and SOPs. Meeting deadlines. Such as deactivated credentials - 543.20(f)(4)

My Notes:



Case 1 – How It Went Wrong

AD (Active Directory)

Network layout

Software Patches

User Controls

Key Points:

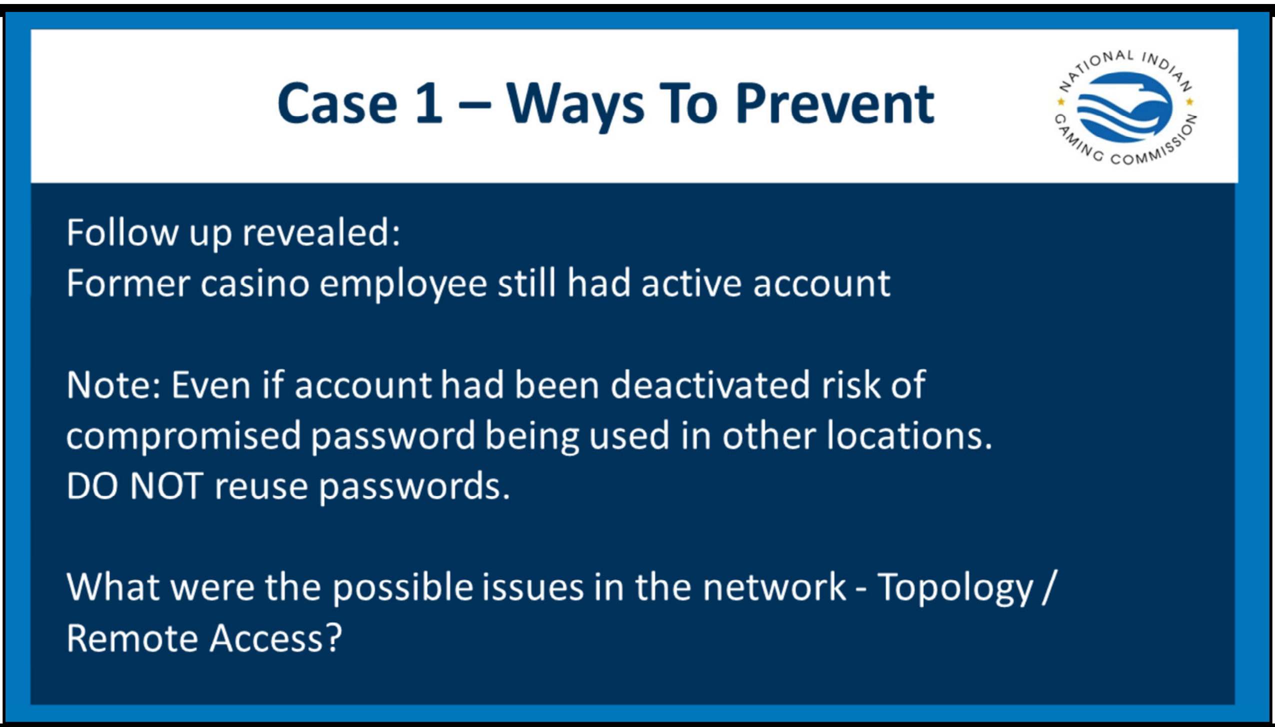
The issues stem from ***more*** than just Active Directory

There were likely issues in the network layout. If sharing same AD systems that means there is a possible connection there either via internal networks or the internet

This was a relatively recent vulnerability, a zero-day vulnerability that ultimately caused the successful attack, but if not that attack, it could easily have been a different attack vector. Stress the importance of software and firmware security updates.

We already covered some of the issues of user control provisioning, but in this case there were specific issues regarding the former employee’s credentials.
This is consistently one of the most common AUP finding areas.

My Notes:



Case 1 – Ways To Prevent

Follow up revealed:
Former casino employee still had active account

Note: Even if account had been deactivated risk of compromised password being used in other locations. DO NOT reuse passwords.

What were the possible issues in the network - Topology / Remote Access?

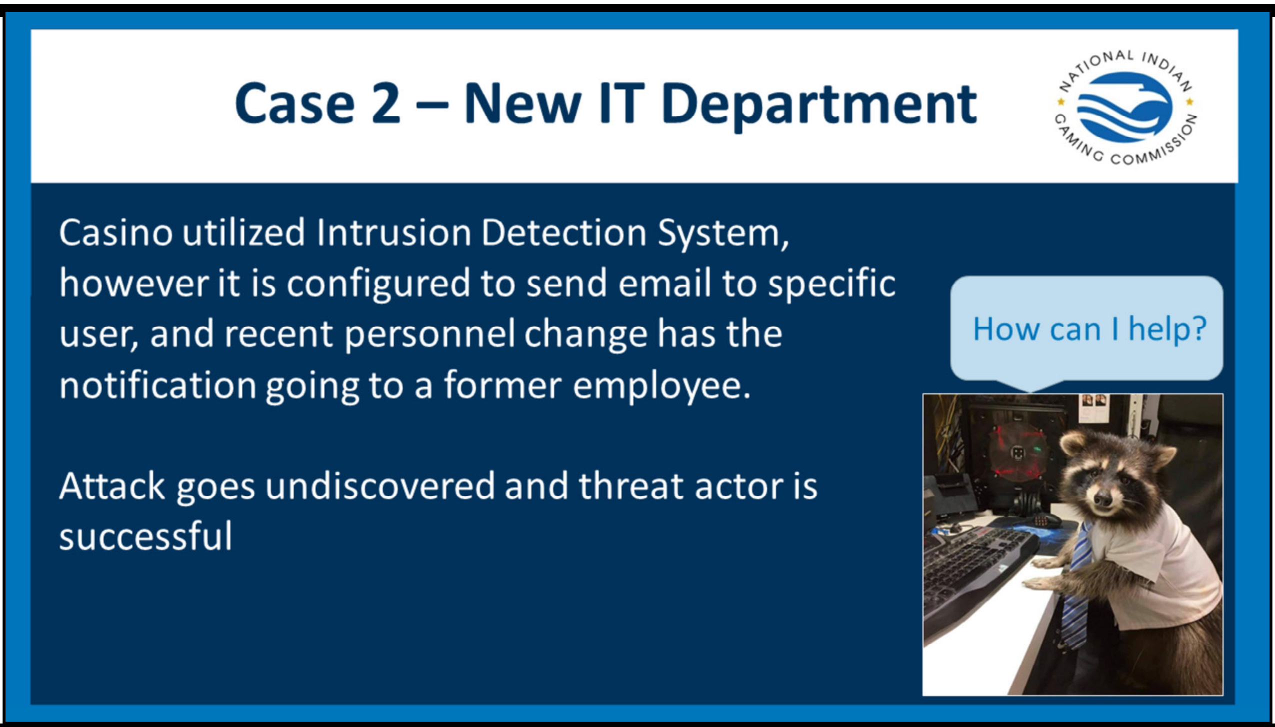
Key Points:

User controls
Passwords - 543.20(f)(1)
Deactivated accounts- 543.20(f)(4)

Logical security: 543.20(e)(2) – Non-essential ports

Remote Access 543.20(h) Issues as well?

My Notes:



Case 2 – New IT Department

Casino utilized Intrusion Detection System, however it is configured to send email to specific user, and recent personnel change has the notification going to a former employee.

Attack goes undiscovered and threat actor is successful

NATIONAL INDIAN GAMING COMMISSION
How can I help?

Key Points:

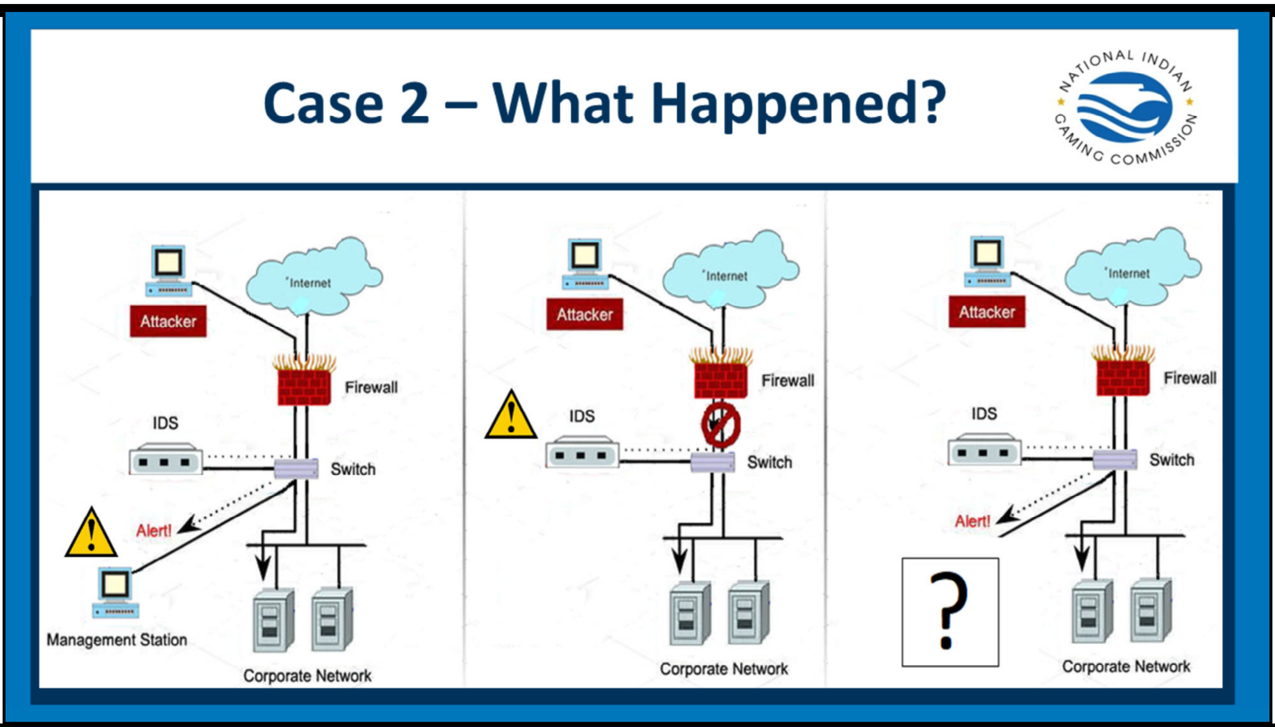
Intrusion detection system is misconfigured to not disable or disconnect suspected malicious device, only to send email to designated IT employee.

Sends email to former employee not to the new staff or to a group address (i.e.. itsupport@casino.com).

Key Terms:

IDS (Intrusion Detection System) – is a device or software application that monitors a network or systems for malicious activity or policy violations

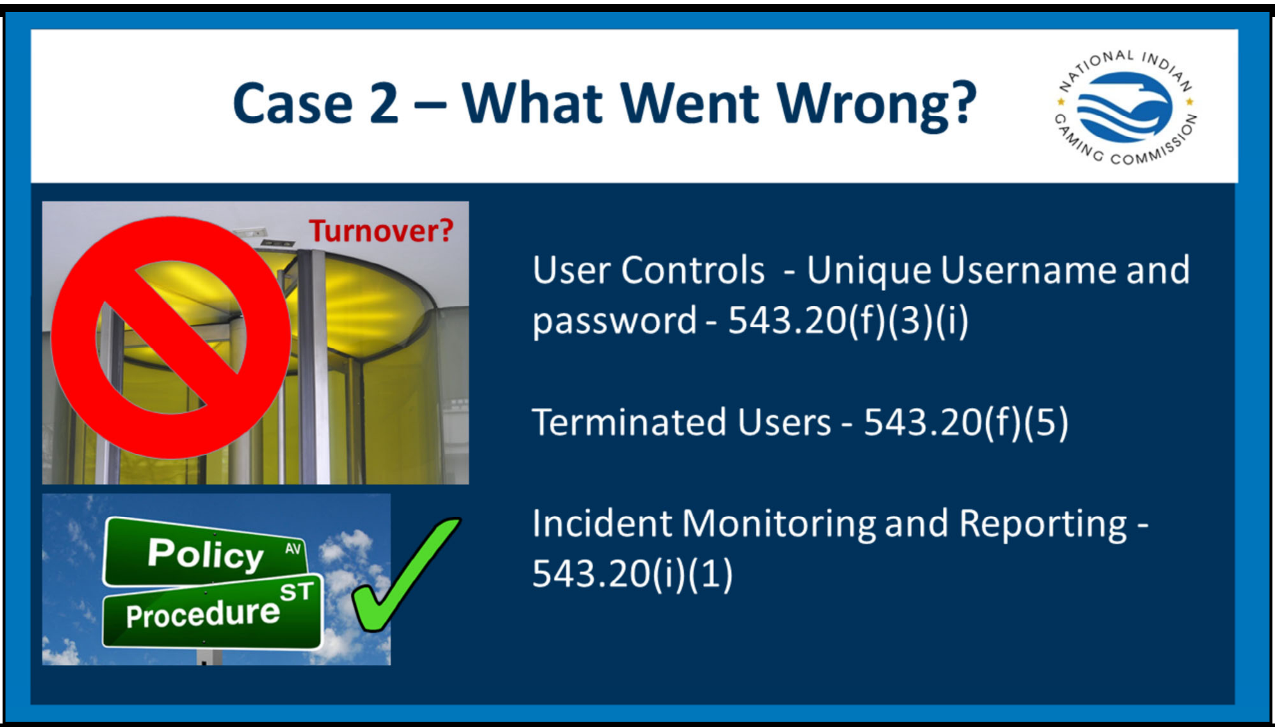
My Notes:



Case 2 – What Happened?

Key Points:

My Notes:



Case 2 – What Went Wrong?

User Controls - Unique Username and password - 543.20(f)(3)(i)

Terminated Users - 543.20(f)(5)

Incident Monitoring and Reporting - 543.20(i)(1)

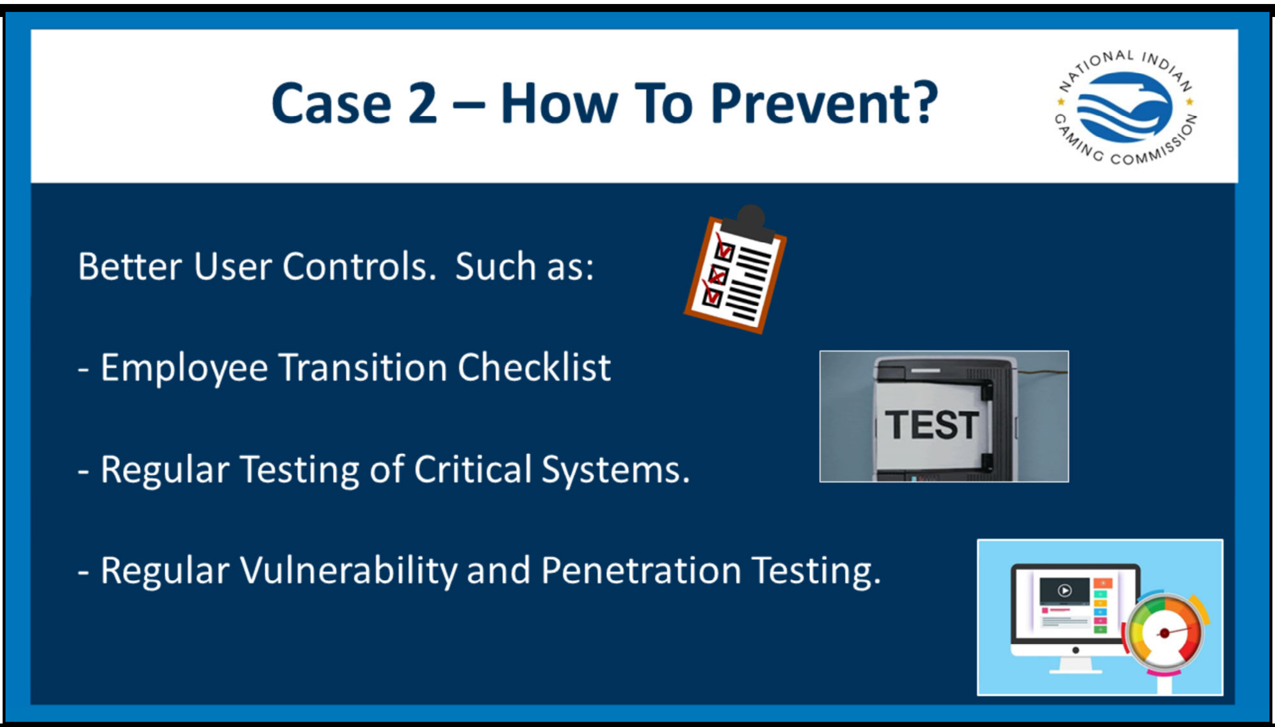
NATIONAL INDIAN GAMING COMMISSION
Turnover?
Policy AV
Procedure ST

Key Points:

- Is this just another case of poor turnover and the “great resignation” of the last couple years?

- Not exactly, this case is a good argument for improved user controls and policies and procedures regarding usernames and passwords and what to do when a user changes departments or leaves

My Notes:



Case 2 – How To Prevent?

Better User Controls. Such as:

- Employee Transition Checklist
- Regular Testing of Critical Systems.
- Regular Vulnerability and Penetration Testing.

Key Points:

Employee Transition (Off boarding) Checklist of all systems, apps, devices, cloud accounts, remote access, etc.

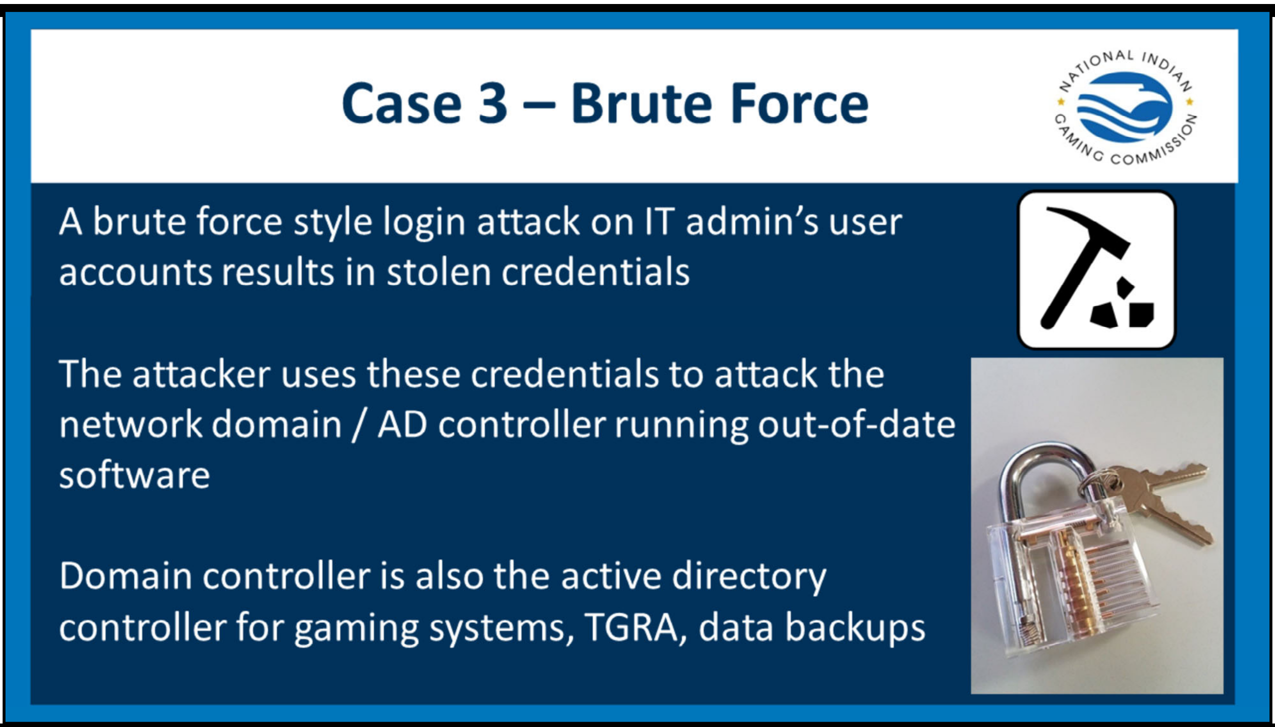
Employee Change management - User controls - Unique UN PW - 543.20(f)(3)(i)

Deactivated users 543.20(f)(5)

Incident monitoring and reporting - 543.20(i)(1) ”Are procedures implemented for responding to, monitoring, investigating, resolving, documenting, and reporting security incidents associated with information technology systems?”

Note: Disaster recovery important but also P&P for transitioning

My Notes:



Case 3 – Brute Force

A brute force style login attack on IT admin's user accounts results in stolen credentials

The attacker uses these credentials to attack the network domain / AD controller running out-of-date software

Domain controller is also the active directory controller for gaming systems, TGRA, data backups

NATIONAL INDIAN GAMING COMMISSION

Key Points:

Attackers are able to steal admin password using a brute force style attack.

The network is configured in such a way that various systems can see and access each other.

Key Terms:

Brute force attack – consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Domain controller - a server computer that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing host access to domain resources. It authenticates users, stores user account information and enforces security policy for a domain. It is most commonly implemented in Microsoft Windows environments, where it is the centerpiece of the Windows Active Directory service.

My Notes:

AD (Active Directory) – is a *directory* service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. While It is perhaps most commonly used to authenticate and authorize users and computers within a Windows domain type network, Active Directory has become an umbrella title for a broad range of directory-based identity-related services.

Case 3 – Zoom Poll

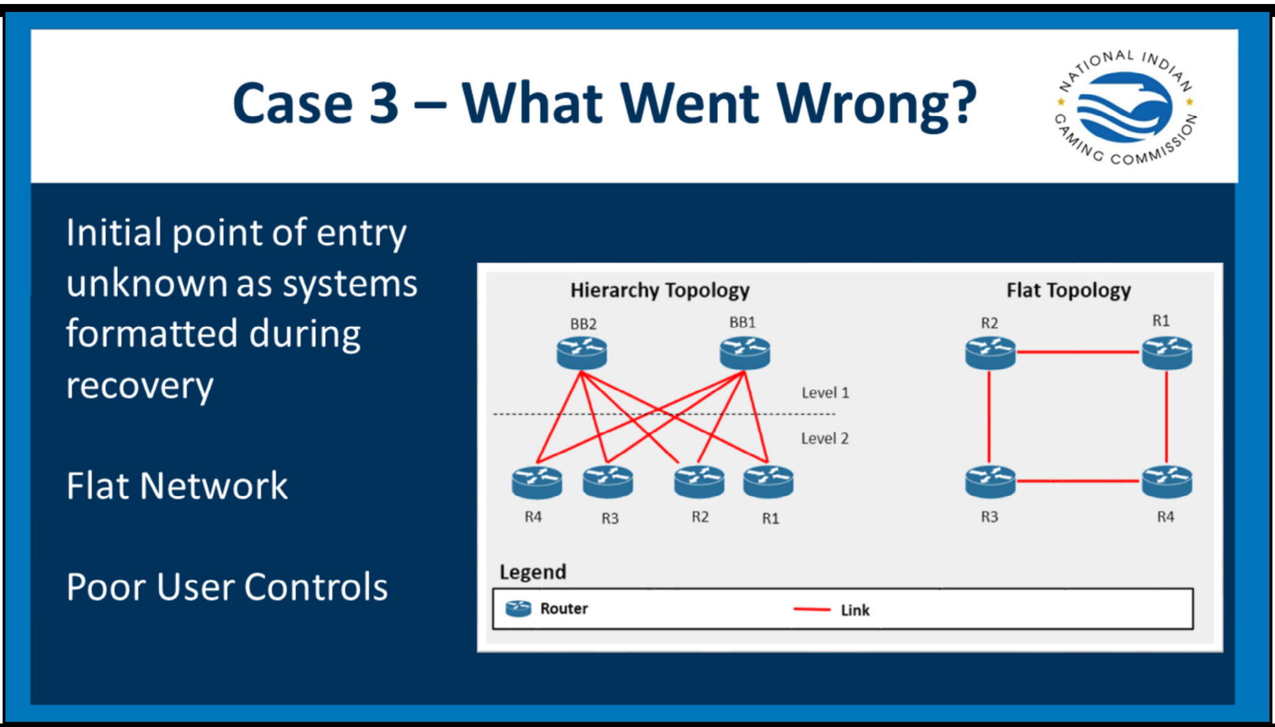
Zoom Poll

Key Points:

Zoom Poll Question: "What do you think were the primary causes?

A. Software update?
B. User controls?
C. Logical security?
D. Something else?

My Notes:



Case 3 – What Went Wrong?

Initial point of entry unknown as systems formatted during recovery

Flat Network

Poor User Controls

Key Points:

- Disaster recovery plan missing, infected systems overwritten not disabled. - Incident monitoring and reporting - 543.20(i)(1)

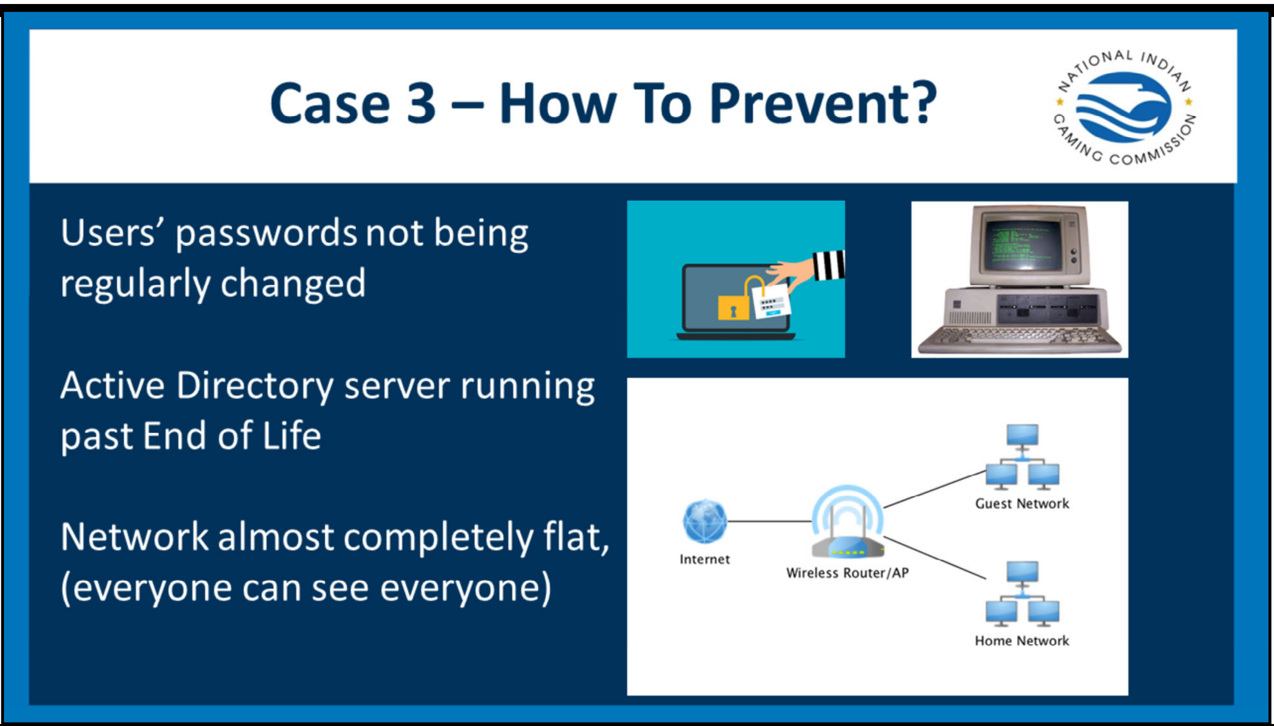
- Network flat (not segregated) - Logical security: 543.20(e)2 – disable non-essential ports

Key Terms:

Flat Network – is a computer network design approach that aims to reduce cost, maintenance and administration. Unlike a hierarchical network design, the network is not physically (or logically) separated using different switches.

Hierarchy Topology – interconnects multiple groups that are located on the separate layers to form a larger network. Each layer concentrates on the specified functions, this allows to choose the right equipment for the layer.

My Notes:



Case 3 – How To Prevent?

Users' passwords not being regularly changed

Active Directory server running past End of Life

Network almost completely flat, (everyone can see everyone)

Key Points:

If you aren't changing your password or only making minor changes it's MUCH easier to crack the password.

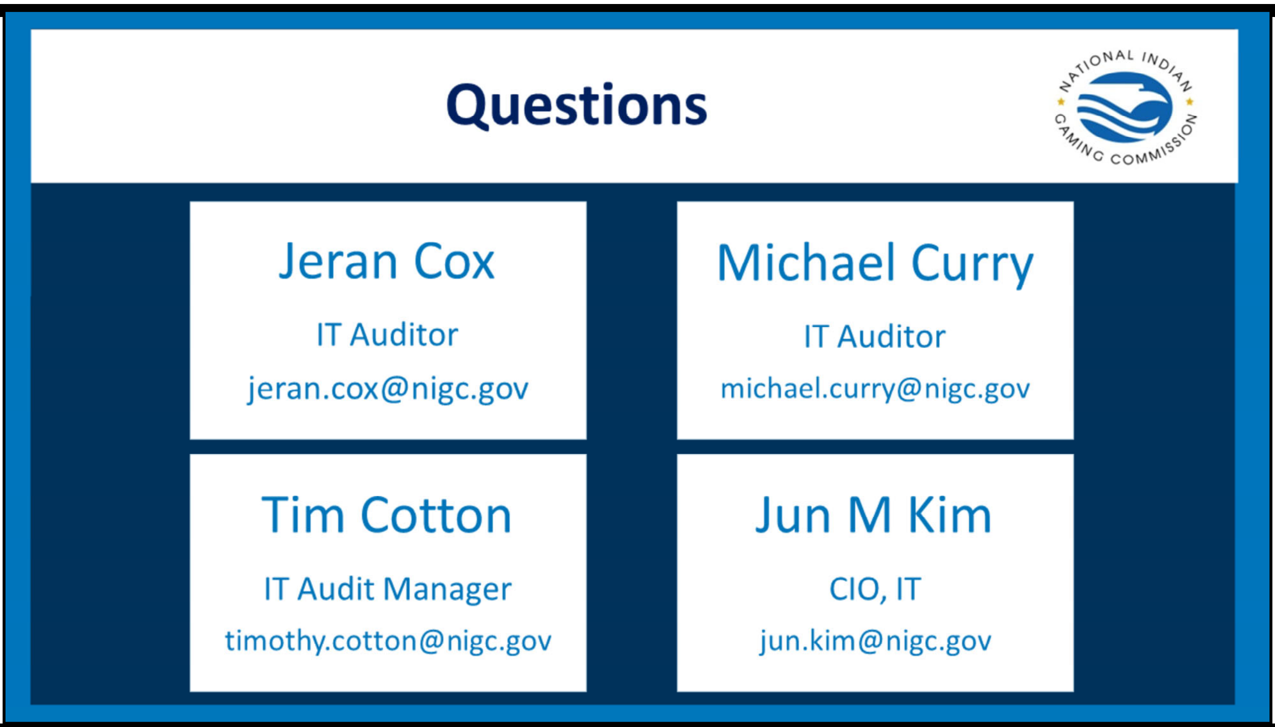
If the system is too old and no longer supported it's much more susceptible to security vulnerabilities

No network segregation, no network hierarchy. Many home network residential use router / AP have the option of a "guest" network that is separate and private, it's best practice to use similar segregated topology strategies in corporate networks.

What were some of the possible compliance violations?

Logical security: 543.20(e)2 – disable non-essential ports
User Controls: 543.20(f)(3)(ii) – Passwords not being changed

My Notes:



Questions

NATIONAL INDIAN GAMING COMMISSION

Jeran Cox
IT Auditor
jeran.cox@nigc.gov

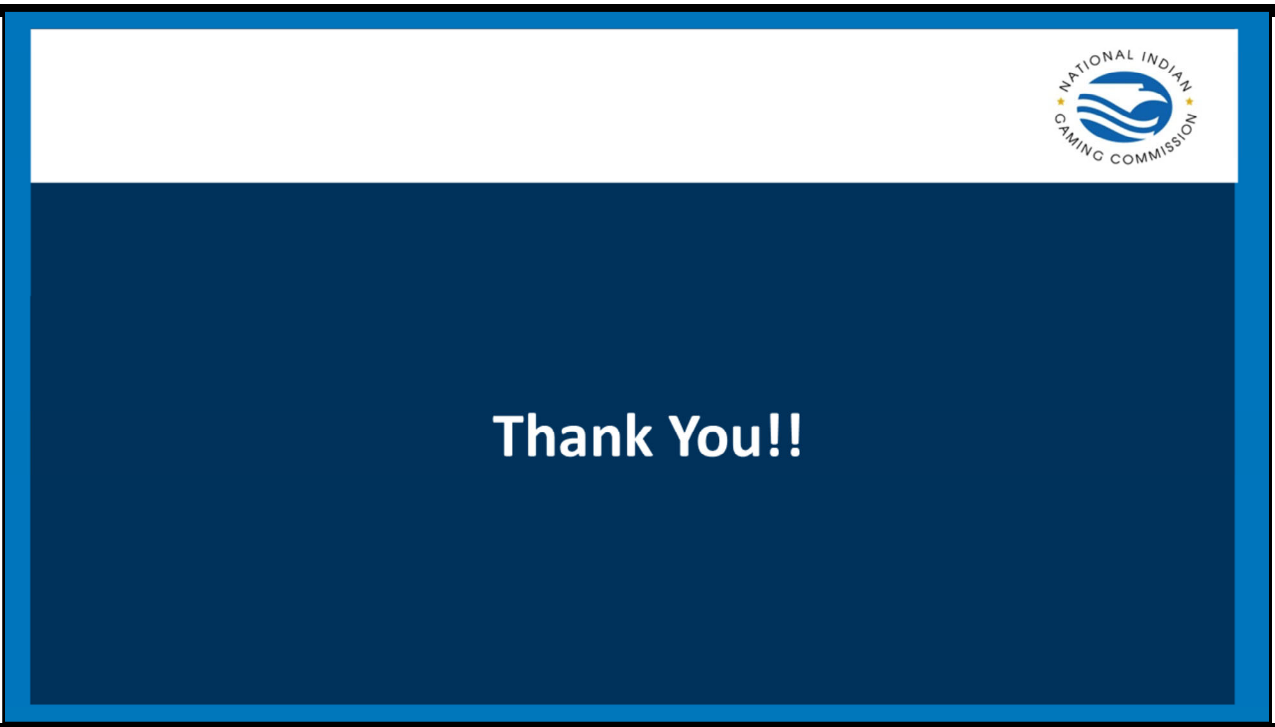
Michael Curry
IT Auditor
michael.curry@nigc.gov

Tim Cotton
IT Audit Manager
timothy.cotton@nigc.gov

Jun M Kim
CIO, IT
jun.kim@nigc.gov

Key Points:

My Notes:



Thank You!!

Key Points:

Thank you for attending.

If you have any questions or comments please send them to TRAININGINFO@nigc.gov

My Notes: