REDISTRICTING SECURITY
Cybersecurity and Infrastructure Security Agency

- Mission: Lead the National effort to understand and manage cyber and physical risk to our critical infrastructure.

- *Defend Today. Secure Tomorrow*
Our Risk Management Approach

1. Partner with the Right People
2. Understand What’s Important
3. Learn the Vulnerabilities
4. Assess Risk and Consequences
5. Promote Controls and Countermeasures
6. Understand What Risk Remains
7. Remain Threat Informed

Matthew Masterson
October 28, 2019
Who Could We Partner with
Understanding the Threat

Hackers penetrate Illinois voter registration database

Source: "Cyber Threats to Canada’s Democratic Process," Canada Centre for Cyber Security
Understanding the Threat

The Cybersecurity 202: The 2020 census could be a prime target for hackers

By: Derek Hemmera
August 6, 2019

The Key

This March 22 photo shows an envelope containing a letter from the Census Bureau mailed to a resident in Providence, R.I., as part of the nation’s test run of the 2020 Census. (Michelle R. Smith/AP)
Objectives of Election Interference

**IMMEDIATE GOAL**
- Affect popularity of candidates
- Call into question legitimacy of election process
- Promote desired election outcome

**MID-TERM GOAL**
- Polarize political discourse
- Weaken confidence in leaders

**LONG-TERM GOAL**
- Promote foreign economic, ideological, military interests
- Reduce confidence in democracy
- Create divisions in international alliances

Source: “Cyber Threats to Canada’s Democratic Process,” Canada Centre for Cyber Security
Cyber Attacks
• Social Engineering
  ▪ Spear-phishing
• Hacking
  ▪ SQL Injection
  ▪ Port scans
  ▪ Man in the Middle (MITM) Attacks
• Distributed Denial of Service (DDoS)
• Ransomware/Wipers

Information Operations
• Leaking stolen information
• Spreading false or misleading information
• Amplifying divisive content
• Interrupting service to public facing online resources
Ransomware

- Ransomware is a type of malicious software designed to deny access to a computer systems or data until a ransom is paid.
- If ransom demands are not met, the system or encrypted data remains unavailable, or data may be deleted.
- In elections this could be used to deny access or delete Voter Registration and/or Vote Tabulation data.
Complex IT Systems are needed to support redistricting efforts:

- Voter Registration Systems
- Servers
- Workstations/Clients
- Networks – Open & Closed
- Tablets
- Smartphones
- Printers
- Copiers
- Fax machines
- VoIP
- GIS interfaces
- Websites
- Software versions
- Vendors
- Contracts
Risk is the potential for an unwanted outcome resulting from an incident, event, or occurrence as determined by its likelihood and the associated consequences and is influenced by:

**Threat/Hazards**
- The greater the threat/hazard, the greater the risk

**Vulnerabilities**
- The more vulnerable you are, the greater the risk

**Consequences**
- The higher the consequences, the greater the risk
This service tracks and reports the vulnerabilities identified for each system scanned and rates the most severe vulnerabilities identified as a “high” or “critical” severity level. While comparing the raw count of vulnerabilities, or vulnerabilities per sector, is statistically misleading, a comparison of the vulnerabilities, averaged per stakeholder group, provides a snapshot in time to compare across stakeholder groups.
The time it takes to mitigate vulnerabilities can be important information about the “health” of a network.

Average time for entities to mitigate vulnerabilities (in days)

- **All**: 102.4 days to mitigate critical, 109.8 days to mitigate high
- **Federal**: 71 days to mitigate critical, 34 days to mitigate high
- **SLTT**: 185.4 days to mitigate critical, 205.3 days to mitigate high
- **EI**: 281.8 days to mitigate critical, 346.9 days to mitigate high
Phishing remains one of the primary attack paths used by threat actors. As part of their assessment offerings, DHS provides focused PCAs. The amount of an organization’s users that click on the DHS phishing email—called user click rates—and the ratio of users that interact with a potentially malicious email can often indicate the success, or lack thereof, of an organization’s user training and awareness.

<table>
<thead>
<tr>
<th>Stakeholder Group</th>
<th>Median percentage of user click rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Election Infrastructure entities</td>
<td>6.15%</td>
</tr>
<tr>
<td>SLTT Government entities</td>
<td>6.91%</td>
</tr>
<tr>
<td>Federal entities</td>
<td>6.05%</td>
</tr>
<tr>
<td><strong>Total user click rate across all assessments</strong></td>
<td><strong>6.71%</strong></td>
</tr>
</tbody>
</table>
## Top Vulnerability Findings Across All Assessments

<table>
<thead>
<tr>
<th>Finding Description</th>
<th>EI Entities</th>
<th>SLTT Governments</th>
<th>Federal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spearphishing susceptibility</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Spearphishing weakness</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Patch management</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Administrator password reuse</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Insecure default configuration</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Clear text password disclosure</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Unsupported operating system or application</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Easily guessable credentials</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Weak password policy</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
With so many factors...

Things that matter

Things you can control

Where you should focus!
...And what is that?

The security of your network
The security of your equipment
The security of your people
Risk Management 101:

ESSENTIALS OF RISK MANAGEMENT:
1. DON'T DO ANYTHING WRONG TODAY.
2. DON'T DO ANYTHING WRONG TOMORROW.
3. REPEAT.

© Randy Glasbergen / Glasbergen.com
Network Security Controls and Countermeasures

Preventative
- Improve Software and Patch Management
- Security Training: All people involved in process should be trained and aware of risks
- Exercise Incident Reporting and response procedures
- Implement Credential Management and Multi-factor authentication
- Secure email and all workstations – access control management

Detective
- Monitor: Intrusion Detection and Netflow Sensors
- Maintain Situational Awareness
- Ensure Auditability
- Centralize Log Management: Update PowerShell and Enable Advanced Logging
- Establish a baseline for Host and Network activity

Corrective
- Promote Backup Policies; Recovery Point Objectives, Recovery Time Objectives
- Have an incident response plan, practice that plan, be prepared to communicate

https://www.us-cert.gov/ncas/tips/ST19-002
Secure the Human- Employees

- Clearly define job descriptions
  - Identify responsibility and authority, particularly for information security issues (e.g. PII, sensitive data, chain of custody, etc.)
  - Have a physical and digital access control policy that fits the job duties
- Conduct background checks
- Require signed agreements, policies, and training
- Have a separation/termination policy
Secure the Human- Vendors & Contractors

- Treat them as employees
- Require background checks
- Provide access only to required areas – physically and logically
- Where applicable require them to sign agreements, policies, and trainings.
- Have a separation policy – both for company and employees
Info Security 101

1. Everyone is a security official - IT Governance
2. Use multi-factor authentication
3. Secure access to critical information
4. Practice cyber hygiene
1. IT Governance

You must create a proactive security culture:

- Lead by example; if necessary collaborate with other Senior Leadership (e.g. CISO, CIO) to express the importance from top-down
- Issue guidance about the necessity of applying security standards
- Conduct training and orientations on policies and procedures
- Review the implementation of policies and procedures by operational staff
- Provide authority and support to implementers that enforce policies and procedures
2. Multifactor Authentication

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

- Multifactor Authentication involves using more than just one method of authenticating an entity
- Two-Factor authentication is regarded as strong authentication

Know
Are
Have
3. Personnel Access Controls

Identify and document dependencies and roles

- Internal dependencies on staff
- Vendor dependencies
- What is risk to your personal systems

Access controls must match roles and responsibilities

- Need to know – least privileged
4. Cyber Hygiene

- Protect your credentials
  - Passwords, key cards, keys, etc.
- Don’t click on links and opening attachments from unknown sources.
- Be wary of unusual activity or notifications
  - Locked out of an account or receive an email saying your password has been changes.
- Avoid clicking on pop-up windows & ads when browsing the internet.
- Software updates fix “bugs” and patch other vulnerabilities.
  - Unpatched software is vulnerable to malicious cyber activity. If you see that software needs to be updated notify IT.
Recommendations to solve most common vulnerabilities

Mitigate Internet Vulnerabilities in a timely manner

- Recommend that EI Subsector entity managers mitigate all internet-accessible high and critical severity level vulnerabilities within 30 days. Vulnerabilities with lower severity levels should be reviewed and either mitigated, or the associated risk formally accepted, within 60 days.

Strengthen Password Policy and Auditing Processes

- Recommend the use of multi-factor password technology. Entities should perform regular audits of their password policy. Password best practices include ensuring that default passwords are never used in production, that strong passwords are required and used, and that administrators use encrypted password vaults.

Implement Network Segmentation

- Internal network architecture should protect and control access to the entity’s most sensitive systems. Recommend that user workstations should be less trusted and connections to external networks should be isolated, controlled, and monitored.

Replace Unmaintainable Equipment

- All EI Subsector equipment should be maintainable with current security patching. Exceptions should be minimized and isolated.
CISA Core Elections Services

Vulnerability Scanning

- A scanning of internet-accessible systems for known vulnerabilities on a continual basis. As potential issues are identified, CISA notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. Conducted remotely and fully automated.

Remote Penetration Testing

- Utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. The assessment simulates the tactics and techniques of malicious adversaries and tests centralized data repositories, externally accessible assets, and web applications.

Phishing Campaign Assessment

- Measures the susceptibility of an organization’s staff to social engineering attacks, specifically email phishing attacks. The assessment takes place during a six-week period. An assessment report is provided two weeks after its conclusion. The assessment report provides guidance, measures effectiveness, and justifies resources needed to defend against and increase staff training and awareness of generic phishing and spear-phishing attacks.

To request services email: NCCICcustomerservice@hq.dhs.gov
Prepare for Ransomware

- **Create Backups**
  - Backup your data regularly
  - Have access to your software and source code in case you need to rebuild the system
- **Test your plans and backups**
- **Develop an Incident Response**
- **Utilize CISA Services (NCCICcustomerservice@hq.dhs.gov)**
  - Remote Penetration Testing (RPT)
  - Vulnerability Scanning