ELECTION CENTER
THE NATIONAL ASSOCIATION of ELECTION OFFICIALS

35th Annual
National Conference
Orlando, FL

2019 Professional Practices Program

Elections Cybersecurity
Risk Assessment & Benchmarking Tool

Cook County, Illinois

Submitted by:

Karen A. Yarbrough, Cook County Clerk
Rahul Patel, Elections Information Security Officer
Ed Michalowski, Deputy Clerk of Elections
Tonya Rice, Director of Elections
69 West Washington, Ste. 500
Chicago, IL, 60602
312-603-0926
tonya.rice@cookcountyil.gov
https://www.cookcountyclerk.com/

Elections Cybersecurity Risk Assessment & Benchmarking Tool
Cook County, Illinois

In the increasingly complex security environment, the Cook County Clerk's Office in conjunction with the Chicago Board of Election Commissioners hired a dedicated Elections Information Security Officer help navigate election cybersecurity issues. Cook County realized a standard cybersecurity risk assessment is necessary for elections officials to identify the gaps in critical risk areas and to determine actions to close those gaps. Therefore, Cook County developed an elections specific cybersecurity risk analysis methodology and Benchmarking Tool to manage cybersecurity risks related with elections systems, processes, and people.

Cook County's innovative Benchmarking Tool is used to clearly define a cyber risk management approach to identify vulnerabilities and implement appropriate security controls. In this professional practice paper, we discuss controls and the methodology for analyzing risk, and for mitigating controls for systems and processes such as Voter databases, Tallying Systems, Communication processes, securing Social Media channels, Vendor Management, and the user behavior. In addition, we present a sample Benchmarking Tool to demonstrate an Elections Security Risk Scorecard based on the Harvard Kennedy School's Belfer Center for Science and International Affairs (HBC) "State and Local Election Cybersecurity Playbook" and Center for Internet Security (CIS) "Handbook for Elections Infrastructure Security".

Methodology

The Benchmarking life cycle used in Cook County is organized in 5 phases with a few steps in each phase. The process is repeated on a yearly basis and aligned with the audit/assessment cycle. It is then followed by the planning and budgeting cycle to ensure remediation efforts are supported with staff, timelines, and funding.

1. Identify and assess the security posture by engaging stakeholders

a. We examine all critical systems – endpoints, network, and web application components – to identify critical cybersecurity gaps.
b. We perform automated as well as manual assessments, analysis, and verification of all identified security gaps and vulnerabilities.
c. We conduct assessments by engaging all stakeholders including election managers, information system owners, application developers and vendors who have knowledge and responsibility for managing specific technology and/or process components.

2. Analyze and Review results

Once the gaps are identified, we create a ranked list of all those gaps and vulnerabilities by considering the following technical aspects:

a. Device Class – How important and what volume of information is handled by the device?
b. Connectedness – Is the device connected to the Internet (High risk), indirectly connected when needed (Medium Risk) or isolated (Low risk)?
c. Probability – What is the probability that the risk will be realized and how easy will it be to exploit the weaknesses or cybersecurity gaps identified?
d. Impact – If the risk is realized how serious will the incident be on the election authority from a Confidentiality-Integrity-Availability (CIA) point of view?

i. Confidentiality – Protecting the information from disclosure to unauthorized parties. What is the impact if confidentiality of the information is breached?
ii. Integrity – Protecting information from being modified by unauthorized parties. What is the impact if integrity of the information is compromised?
iii. Availability – Ensuring that authorized parties can access the information when needed. What is the impact if the information is not available?

3. Benchmark the cybersecurity risk using the tool

In Cook County, we take a point-in-time Benchmark of our cybersecurity posture and prioritize remediation process with this Benchmark. We developed a simple Benchmarking Tool, which can be used by any sized county at no additional cost, to capture current posture, major gaps /vulnerabilities, overall score, and the improvement from the last assessment cycle (see Attachments). We identify gaps within the technical and functional areas.

a. Technical area - Devices, Processes, Software, Users, and Transmission.
b. Functional area - Voter Registration Databases (VRDB), Voter Check-ins (ePollbooks), Vote Casting Devices, Ballot Files, Election Management System (EMS)/Vote Tallying System, Election Night Reporting, Communications, Social Media, and Vendor Management.

We benchmark the assessment on a pre-defined scale: met the requirement (4 points), partially met (1, 2 or 3 points), or did not meet requirement (0 points). A subtotal and a percentage (achieved score / maximum possible) score provide a snapshot of where we stand for each specific area.

4. Implement improvement plan

With benchmarking, we have a clear picture of where the most effort is needed. Cook County's security team and senior elections management team meets regularly to ensure awareness and visibility for all efforts. We develop actionable improvement plans based on the following criteria:

a. Functional priority – How important is the function to the elections process?
b. Major risk – How large is the cybersecurity gap identified earlier?
c. Cost/Benefit – What is the best remediation outcome per dollar spent?
d. Skillset needed – What is the most effective use of all available expertise?
e. Time needed – Which combination of short, small-win and long, big-win efforts will ensure a continuing realization of benefits?

5. Repeat to find new opportunities to improve

Cook County follows a yearly Plan-Do-Check-Act-Adjust cycle following by posture assessment and monitoring. In each cycle, we seek to address new risks and work in progress carried over from the previous cycle. We also consider new technological capabilities that can be used to address risks more effectively, with automation, and/or with lesser investments.

Summary

Cook County uses an internally developed Benchmarking Tool based on CIS and Harvard Belfer Center's recommendations. This approach benefits us by providing consistent and systematic processes for identifying and prioritizing security efforts. It also helps allocate resources and plan for multiple security efforts based on priorities and gaps. Since the tool is elections specific, it provides snapshots of risks and required remediation efforts specifically related to election systems and functions. The Benchmarking Tool is also an effective means of communicating the cybersecurity risk posture and tracking progress over time.

Attachment 1

Cook County Clerk, Sample Gap Analysis - CIS

	A	B	C	D	E	F	G	H	I
1	Number	Control	Asset Class	Connectedness Class	Priority	Met Control?	Score	Gap	Max Possible Score
2	1	Whitelist which IPs can access the device	Devices	Network Connected	High	Yes	3	0	3
3	2	Regularly scan the network to ensure only authorized devices are connected	Devices	Network Connected	High	Yes	3	0	3
4	3	Limit the devices that are on the same subnet to only those devices required	Devices	Network Connected	High	No	0	3	3
5	4	Only utilize approved and managed USB devices with appropriate device encryption and device authentication	Devices	Network Connected	High	Partial	1	2	3
6	5	Disable Wireless Peripheral Access (Bluetooth, WiFi, radio, microwave, satellite, etc.) Unless Required	Devices	Network Connected	High	Partial	2	1	3
7	6	Ensure the system is segregated from other independent election systems and non-election supporting systems	Devices	Network Connected	High	Yes	3	0	3
8	7	Deploy Network Intrusion Detection System (IDS) (e.g., MS-ISAC Albert sensor) on Internet and extranet DMZ systems	Devices	Network Connected	High	Yes	3	0	3
9	8	If wireless is required, ensure all wireless traffic use at least Advanced Encryption Standard (AES) encryption with at least Wi-Fi Protected Access 2 (WPA2)	Devices	Network Connected	High	Yes	3	0	3
10	9	Use trusted certificates for any publicly-facing website	Devices	Network Connected	High	Partial	1	2	3
11	27	Ensure that all devices are documented and accounted for throughout their lifecycle	Devices	Network Connected	Med	Yes	2	0	2
12	28	Utilize tamper evident seals on all external ports that are not required for use and electronically deactivate ports where feasible	Devices	Network Connected	Med	Yes	2	0	2
13	29	Maintain an inventory of assets that should be on the same subnet as the election system component	Devices	Network Connected	Med	Yes	2	0	2
14	30	Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal	Devices	Network Connected	Med	Yes	2	0	2
15	31	Conduct load and stress tests for any transactional related systems to ensure the ability of the system to mitigate potential DDoS type attacks	Devices	Network Connected	Med	Yes	2	0	2
16	55	For data transfers that utilize physical transmission, utilize tamper evident seals on the exterior of the packaging	Device	Indirectly Connected	High	Yes	3	0	3
17	56	Disable wireless peripheral access of devices	Device	Indirectly Connected	High	Partial	2	1	3
18	67	Utilize tamper evident seals on all external ports that are not required for use	Device	Indirectly Connected	Med	Yes	2	0	2
19	68	Ensure that all devices are documented and accounted for throughout their lifecycle	Device	Indirectly Connected	Med	Yes	2	0	2
20	69	Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal	Device	Indirectly Connected	Med	Yes	2	0	2
21			Device				40	9	49
22	10	Ensure logs are securely archived	Process	Network Connected	High	Yes	3	0	3
23	11	On a regular basis, review logs to identify anomalies or abnormal events	Process	Network Connected	High	Yes	3	0	3
24	12	Ensure critical data is encrypted and digitally signed	Process	Network Connected	High	Partial	2	1	3
25	13	Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines	Process	Network Connected	High	Yes	3	0	3
26	14	Perform system testing prior to elections (prior to any ballot delivery), such as acceptance testing	Process	Network Connected	High	Yes	3	0	3
27	15	Ensure acceptance testing is done when receiving or installing new/updated software or new devices	Process	Network Connected	High	Yes	3	0	3
		Conduct criminal background checks for all staff including vendors, consultants, and							

CIS | CIS Graph | HBC | HBC Graph

Class	Score	Gap	% Meet
Device	40	9	81.63%
Process	48	4	92.31%
Software	46	5	90.20%
Users	40	10	80.00%
Transmission	11	3	78.57%
	185	31	85.65%

Attachment 2

Cook County Clerk, Sample Gap Analysis - HBC

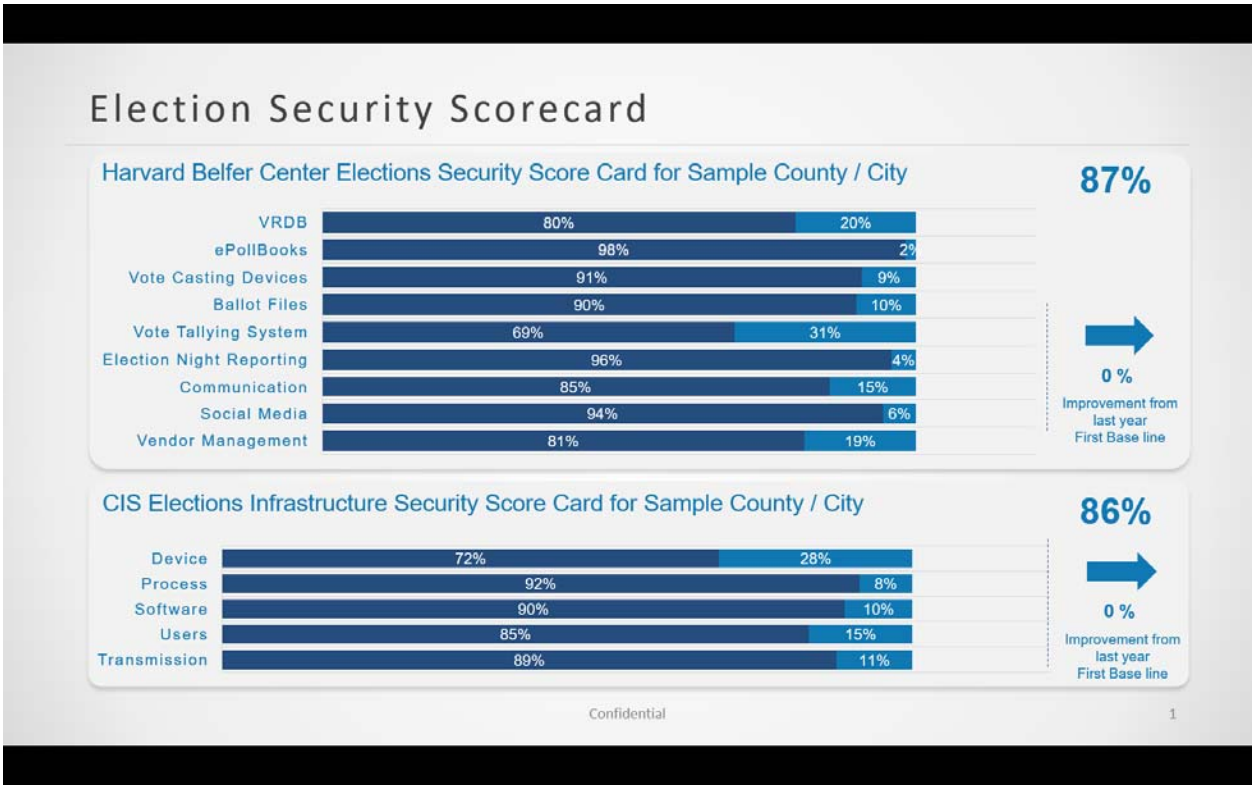
	A	B	C	D	E	F	G
1	VRDB	Type	Control	Effective	Score (Yes, Partial, No, N/A)	Gap	Maximum Score
2	VRDB	Identify	Map how other systems connect to the VRDB.	Yes	4	0	4
3	VRDB	Identify	Know where the VRDB is hosted	Yes	4	0	4
4	VRDB	Identify	Know what accounts have access and what level of access each account has	Yes	4	0	4
5	VRDB	Identify	Determine which of the servers can be accessed over the Internet	Yes	4	0	4
6	VRDB	Protect	Require strong passwords and implement two-factor authentication	No	0	4	4
7	VRDB	Protect	Conduct penetration tests, source code audits, and encourage vulnerability discovery efforts	Partial	2	2	4
8	VRDB	Protect	Apply software updates and patches	No	0	4	4
9	VRDB	Protect	Ensure that your underlying database server is not accessible over the Internet	Yes	4	0	4
10	VRDB	Protect	Restrict external systems' access to the VRDB.	Yes	4	0	4
11	VRDB	Protect	Log changes	Yes	4	0	4
12	VRDB	Protect	Limit account access to the VRDB	Partial	2	2	4
13	VRDB	Protect	Permissions Management for VRDB accounts	Partial	2	2	4
14	VRDB	Protect	Require users to access the VRDB portal using a VPN	Partial	2	2	4
15	VRDB	Detect	Monitor activity against a baseline and investigate anomalies	Yes	4	0	4
16	VRDB	Detect	Incorporate a human review into data change monitoring to augment technical monitoring	Yes	4	0	4
17	VRDB	Detect	Monitor permission changes	Partial	3	1	4
18	VRDB	Respond	If the incident involved an attacker gaining access to VRDB, perform a thorough review of the system's accounts and access controls	N/A	4	0	4
19	VRDB	Respond	If a physical machine was compromised, disconnect the machine from the network and seek professional forensic assistance.	N/A	4	0	4
20	VRDB	Recover	Execute the recovery plan	N/A	4	0	4
21	VRDB	Recover	Practice restoring from VRDB backups	Yes	4	0	4
22	VRDB	Recover	Lessons learned	N/A	4	0	4
23	**VRDB**				**67**	**17**	**84**
24	ePollBooks	Identify	Examine all the possible functionalities of the device and identify the components you intend to use	Yes	4	0	4
25	ePollBooks	Identify	Know what kind of network connections your e-Pollbooks need	Yes	4	0	4
26	ePollBooks	Identify	Understand how voter information is loaded onto the e-Pollbooks	Yes	4	0	4
27	ePollBooks	Protect	E-Pollbooks should be single-purpose devices	Yes	4	0	4
28	ePollBooks	Protect	Verify the integrity of the e-Pollbook file.	Yes	4	0	4
29	ePollBooks	Protect	Ensure all devices are updated and patched	Yes	4	0	4
30	ePollBooks	Protect	Esure protective measures are in place for internet connecte ePollbooks	Partial	3	1	4
31	ePollBooks	Protect	Have a paper backup	Yes	4	0	4
32	ePollBooks	Protect	Ensure physical security	Yes	4	0	4
33	ePollBooks	Detect	Monitor data changes	Yes	4	0	4
34	ePollBooks	Detect	Perform vulnerability scans	Yes	4	0	4

CIS | CIS Graph | **HBC** | HBC Graph

Class	Score	Gap	% Meet	% Gap
VRDB	67	17	79.76%	20.24%
ePollBooks	55	1	98.21%	1.79%
Vote Casting Devices	40	4	90.91%	9.09%
Ballot Files	36	4	90.00%	10.00%
Vote Tallying System	25	11	69.44%	30.56%
Election Night Reporting	46	2	95.83%	4.17%
Communication	41	7	85.42%	14.58%
Social Media	34	2	94.44%	5.56%
Vendor Management	26	6	81.25%	18.75%
Overall	370	54	87.26%	12.74%

Attachment 3

Cook County Clerk, Sample Cybersecurity Benchmarking Tool



Attachment 4

References

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). (2019). Elections Resources. https://www.cisecurity.org/elections-resources/

The National Protection and Programs Directorate - Department of Homeland Security (2019). Election Security Resource Library. https://www.dhs.gov/publication/election-security-resource-library

The Belfer Center for Science and International Affairs (2018). The State and Local Election Cybersecurity Playbook. https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

The National Science and Technology Institute –U.S. Department of Commerce (2017). NIST Special Publication 800-12r1 – An Introduction to Information Security. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf