Shorenstein Center on Media, Politics and Public Policy

May 2018

Campaign 2018:
Improving Cyber Literacy in Political Campaigns

By Donna Brazile, Joan Shorenstein Fellow, Fall 2017
Former Democratic National Committee interim chair
and adjunct professor at Georgetown University

HARVARD Kennedy School
SHORENSTEIN CENTER
on Media, Politics and Public Policy

Table of Contents

1. Introduction 3
2. Background: The 2016 Election and its Aftermath 4
3. The Challenge in Western Democracies 5
4. The 2018 U.S. Midterm Elections: Are We Ready? 6
5. Social Media Platforms: The Big Unknown 7
6. Are Campaigns Equipped To Maintain Cyber Safety? 9
7. Conclusion 15
8. Acknowledgments 16
9. Appendix: A Survey of Campaign Staff 17

"There should be no doubt that Russia perceives its past efforts as successful and views the 2018 U.S. midterm elections as a potential target for Russian influence operations."

—Dan Coats, Director of National Intelligence, February 13, 2018.

Introduction

The 2016 presidential election was unlike any other. The contest had the look of a circus, with each news cycle driven by outrageous claims and scandalous events rather than an examination of the issues facing the nation. As a result, some voters didn't know who to believe or trust and stayed home on Election Day. The result was an election where the candidate who won the highest office in the land did not win the popular vote.

Since then we have come to know how much our fears and yearnings were manipulated by agents for the Russian government, and how few protections we have in place to prevent them from distorting our electoral process in the coming 2018 midterm elections and the 2020 presidential contest. The hacking of our electoral system poses a significant threat to our democracy by undermining faith in our public institutions such as the mainstream media, political parties, and statewide election systems and databases.

There was a time when, if a foreign power interfered in an American election, both major political parties would spring into action to protect the integrity of our election. That is not happening, and a 2017 Shorenstein Center survey of campaign managers and campaign staff members revealed how unprepared our political candidates are for the digital threats they face at election time. The results show that while those surveyed are aware of the cyber threats, many of them do not take them seriously.

The survey of nearly forty Republican and Democratic campaign operatives, administered through November and December 2017, revealed that American political campaign staff — primarily working at the state and congressional levels — are not only unprepared for possible cyber attacks, but remain generally unconcerned about the threat. The survey sample was relatively small, but nevertheless the survey provides a first look at how campaign managers and staff are responding to the threat.

The overwhelming majority of those surveyed do not want to devote campaign resources to cybersecurity or to hire personnel to address cybersecurity issues. Even though campaign managers recognize there is a high probability that campaign and personal emails are at risk of being hacked, they are more concerned about fundraising and press coverage than they are about cybersecurity. Less than half of those surveyed said they had taken steps to make their data secure and most were unsure if they wanted to spend any money on this protection.

Campaign officials should understand that their key assets in political campaigns, data and technologies, are at risk. Campaign staff, volunteers, and candidates should receive

cyber education training. Our democracy is at risk. Cyber threats are constantly evolving, especially through the use of social media platforms. These "active measures," if not countered through training and a public education campaign, will erode confidence in the U.S. political system, destabilize campaigns, discredit candidates, and weaken both campaigns and election systems through deception, intraparty discord, and the spread of false information.

Background: The 2016 Election and its Aftermath

On January 16, 2017, U.S. intelligence agencies concluded that "Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S Presidential election." The goal, said the agencies, was to "undermine faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency."

Nearly a year later, on February 16, 2018, Special Counsel Robert Mueller, who has been investigating Russian interference in the 2016 election, filed an indictment against 13 Russian nationals and 3 Russian organizations, which sought a specific outcome to the 2016 presidential election. The 37-page indictment reads like a spy novel with Russians posing as Americans to scout out our politics, setting up fake identities and shell companies to pay for demonstrations and rallies, and creating websites and bots that promoted then-candidates Donald Trump, Bernie Sanders, and Jill Stein.

The Democratic National Committee (DNC), along with the presidential campaign of Hillary Clinton (HFA), the Democratic Congressional Campaign Committee (DCCC), and private individuals — plus other entities with the responsibility for keeping statewide databases, voter registration, and electronic poll books — became the targets of a sophisticated cyber hacking operation that sought to sow discord, weaponize hacked emails, create chaos at the ballot box, and undermine faith in the integrity of the election and its outcome.

As Americans prepare for the 2018 midterm election, where there are 435 seats in the U.S. House of Representatives, 34 Senate seats, and 36 gubernatorial seats up for grabs, neither President Donald Trump nor Congress has fully acknowledged the assault on American democracy nor taken credible steps to protect, educate, and prepare American voters on Russian threats to future elections.

President Trump continues to label each investigation into the Russian meddling as a "witch hunt" or "a total hoax" created by his opponents. He refuses to accept the findings of the intelligence agencies. Trump appears unbothered by the threat posed by Russia's attack on our democracy, even as we learn more about its efforts to divide our country and create chaos. In response to the Mueller indictment, Trump issued not a call to action, but a vindication of himself. He tweeted, "Russia started their anti-US campaign in 2014, long before I announced that I would run for President. The results of the election were not impacted. The Trump campaign did nothing wrong — no collusion!"

Both houses of Congress have undertaken investigations into Russian interference in the 2016 presidential election. On April 27, 2018, the House Intelligence Committee concluded its yearlong investigation and issued a report that declared that the Trump campaign did not collude with Russia or aid in Russia's meddling in the presidential election. The Senate's investigation remains ongoing. To date, legislation to address Russia's intrusions remain in their formative, initial stages. However, a bill imposing new sanctions on Russia for its behavior in the Ukraine and its meddling in the 2016 election passed the House 419-3 on July 25, 2017. Democrats have introduced the Election Security Act (on February 14, 2018 in the U.S. House) to help states restore the integrity and privacy of our elections. The law provides grants to states to enable them to update and secure their election infrastructure, but so far it has little to no support from Republicans.

Meanwhile, several states are taking actions to upgrade their electronic voting systems, electronic poll books, and the like to protect against malicious hardware and software vulnerabilities. During the summer of 2017, the National Council of State Legislators (NCSL) convened a major conference to discuss steps to protect the electoral integrity of their systems. One of their recommendations is the creation of a Cybersecurity Task Force to ensure state lawmakers are acutely aware of the threat posed to future elections. NCSL is working closely with the Department of Homeland Security (DHS) to build cyber literacy among state officials and to train state election officials.

With evidence continuing to mount that Russia did indeed attempt to influence the 2016 election, coordination continues to lag at both the federal and state levels where election administration is managed.

The Challenge in Western Democracies

During his testimony to Congress in June 2017, former FBI Director James Comey warned, "it's not a Republican thing or a Democratic thing. It really is an American thing." Comey added, "They're going to come for whatever party they choose to try and work on behalf of, and they're not devoted to either, in my experience. They're just about their own advantage and they will be back."

The United States is not alone in being under attack. The tactics used by the Russians in the United States were perfected after earlier efforts to meddle in the elections of other Western democracies. Within the European Union (EU), Russia has been accused of directly and indirectly engaging in a surreptitious, continent-wide effort to undermine pro-European groups, particularly in the Ukraine and France. Russia's state-owned media have constantly lauded the efforts of far right, anti-EU political parties including those in Holland, France, Germany, and most recently in Austria. The Russian disinformation campaign continues to amplify stories harmful to political leaders and parties that are strongly in favor of the European Union, NATO, and other pro-Western groups.

The U.S. has seen "initial signs" of Russian "subversion and disinformation and propaganda" in the Mexican presidential campaign. In this context, then-National Security Adviser H.R. McMaster said: "…with Russia we are concerned, increasingly concerned, with these sophisticated campaigns of subversion and disinformation and propaganda, the use of cyber tools to do that." According to a clip of his speech obtained by José Díaz Briseño, *Reforma*'s U.S. correspondent, McMaster said: "As you've seen this is a really sophisticated effort to polarize democratic societies and pit communities within those societies against each other and create crises of confidence and to undermine the strength within Europe. You see this most recently with the Catalonia independence referendum in Spain, for example. You see actually initial signs of it in the Mexican presidential campaign already."

Former President George W. Bush has repeatedly spoken out on the dangers of Russian interference. According to a *USA Today* report, Bush stated, "It's problematic that a foreign nation is involved in our election system. Our democracy is only as good as people trust the results."

The 2018 U.S. Midterm Elections: Are We Ready?

In 2018, American voters will go back to the polls to elect 36 governors, 34 U.S. Senators and 435 members of the U.S. House of Representatives. The integrity of our electoral system remains vulnerable to attack. The stakes are high.

Jeh Johnson, former director of the Department of Homeland Security, stated that the U.S. was "on alert on Election Day and in the days leading up to it, along with the FBI." Johnson commented that "…33 states and 36 cities and counties came to the Department before the 2016 election to seek their cybersecurity assistance. In working with those states, DHS helped to address a number of vulnerabilities in election infrastructure." He added, "I'm concerned that we are almost as vulnerable perhaps now as we were six, nine months ago."

One way to prepare for the upcoming elections is to provide state and local election officials with resources to address threats to IT systems and voting technology. In 2017, the House Democrats launched an Election Security Task Force headed by Representatives Bennie Thompson (D-MS) and Robert Brady (D-PA). They issued a report that identified ten specific recommendations on what the federal government and states can and should be doing to secure our nation's elections.

The Secure Elections Act was introduced on December 21, 2017, in the U.S. Senate by a bipartisan group of lawmakers led by Senators James Lankford (R-OK), Amy Klobuchar (D-MN), Lindsey Graham (R-SC), Kamala Harris (D-CA), Susan Collins (R-ME) and Martin Heinrich (D-NM). The Secure Elections Act would mandate DHS to share more information with state and local election officials about threats to their IT systems or voting machines. The bill would also set up an expert panel to draft voluntary risk management guidelines and best practices that state and local agencies can use.

Finally, it would authorize a $386 million grant program to help states implement these guidelines and replace outdated electronic voting machines.

In addition, The Securing America's Voting Equipment (SAVE) Act was introduced on October 31, 2017, by Senators Susan Collins (R-ME) and Martin Heinrich (D-NM). In a press release accompanying introduction of the legislation, the Senators noted that "[i]ntelligence assessments that Russian actors targeted state election voting centers and state-level voter registration databases as part of Russia's larger hostile effort to interfere in last year's election demonstrate a vulnerability to future cyber-attacks and manipulations by foreign hackers in our democratic process. The SAVE Act would facilitate information sharing with states, provide guidelines for how best to secure election systems, and allow states to access funds to develop their own solutions to the threats posed to elections."

In January 2018, all Democratic members of the House Committee on Oversight and Government Reform sent a letter asking Chairman Trey Gowdy to issue a subpoena to finally compel the Department of Homeland Security (DHS) to produce documents it has been withholding from Congress for months related to Russian government-backed efforts to monitor, penetrate, or otherwise hack at least 21 state election systems in the 2016 election. DHS has failed to provide the requested information, but the agency has confirmed that Russia was behind the attacks.

Social Media Platforms: The Big Unknown

It's clear from recent revelations that Russian meddling on social media platforms like Google, Facebook, and Twitter was extensive during the 2016 election. Whether it swayed the election is a hard question to answer, but what we do know is that millions — and potentially tens of millions — of American voters were exposed to content pushed by Russia in an election that was decided by just tens of thousands of votes. And it hasn't stopped, meaning its effect on 2018 and 2020 could be just as pernicious.

Social media platforms have been slow to acknowledge the situation and, until recently, reluctant to do anything about it. In some cases, their policies and actions may have caused valuable information to be lost about the Russian attacks, which often aimed to divide America on race, guns, immigration, religion, and other issues.

As detailed in *Politico*, Twitter was one of the most effectively exploited weapons by the Russian government to undermine Hillary Clinton's campaign and to help Donald Trump in the 2016 race. Kremlin-backed operatives used targeted ad buys, fake users, and automated bots to spread disinformation and false stories. Even so, Twitter's privacy policies for consumers may have resulted in the loss of tweets and data that would be invaluable to investigators trying to see how the Russian operation was carried out. Twitter failed to crack down on suspicious activity, and then allowed the data about that activity to be lost.

Senator Mark Warner, the ranking Democrat on the Senate Intelligence Committee that is investigating Russian interference, said Twitter's response had been "inadequate." According to Senator Warner, Twitter did only the bare minimum of investigating when it came to looking into the activity of the Russians on their platform.

As reported in *The New York Times*, members of the Congressional Black Caucus are just as angry about Facebook's response. Caucus Chair Cedric L. Richmond (D-LA) stated that "[the Caucus] needed Facebook to understand that they [Facebook] play a role in the perception of African-Americans."

Russian-backed operatives made substantial ad buys on Facebook that were aimed at inflaming racial and political divisions at a time when members of the African-American community were trying to highlight problems of systemic racism in the nation's justice system. Meanwhile, the foreign actors were using targeted Facebook ads to make white voters hostile to African-Americans' message and to exploit racial tension and mistrust.

The Senate Intelligence Committee summoned attorneys for Twitter, Facebook, and Google for a public hearing on November 1, 2017, to discuss how Russia may have used their sites to influence the 2016 election. The issue became more pressing for legislators in March 2018 after it was revealed that the personal data of millions of Facebook users was improperly shared with the political data firm Cambridge Analytica, which, in turn, used that data to advance President Trump's campaign. Mark Zuckerberg, CEO and Chairman of Facebook, was called to testify before the Senate Committee on the Judiciary and the Senate Committee on Commerce, Science and Transportation.

Zuckerberg appeared before the joint Senate Committee on April 10, 2018, and testified that Facebook "didn't do enough" to prevent misuse of its platform during the 2016 election. Zuckerberg elaborated: "That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here."

Zuckerberg further testified that Facebook "should have spotted Russian interference earlier," and that it is taking steps to prevent future interference by hostile foreign actors. Zuckerberg's contrition and the fact that Facebook appears serious about making changes to its security and advertising policies are critical first steps to preventing misuse of the social media site in future U.S. elections.

Prior to Zuckerberg's hearing, Senators Warner (D-VA), McCain (R-AZ), and Klobuchar (D-MN) introduced the Honest Ads Act that aims to "prevent foreign interference in future elections and improve the transparency of online political advertisements." Days before his Senate hearing, Zuckberberg endorsed the Act and Twitter soon followed. This legislation is important for the preservation of our democracy because it will inhibit foreign powers from polluting the internet with fabricated stories and disinformation.

Faced with the president's denial and the sluggish response by the tech community, it's more vital than ever that Congress step into the void to raise the alarm and to apply pressure to social media companies through the current Russia investigations and possible legislative remedies.

Are Campaigns Equipped To Maintain Cyber Safety?

Over the past year, the world has become increasingly aware of the importance of cybersecurity for political systems and governments. From Russian infiltration of the 2016 presidential elections in the U.S., to emails from top political leaders leaked to the public, political operatives must be better prepared to protect the integrity of online data and information.

How Do Campaign Staffers View This Threat?

After the hacking of the 2016 election, it's not surprising that nearly all the campaign staff surveyed (92%) were familiar with news about cyber meddling in political campaigns and party offices during the 2016 election cycle. Nearly two-thirds are aware of the practice of fraudulent emails sent under the guise of a trusted colleague to gather confidential information from targeted individuals (known as spear phishing). Perhaps the most famous example of spear phishing was the hacking of Hillary Clinton campaign chairman John Podesta's emails.

Figure 1. Familiarity with 2016 Campaign Cyber Meddling

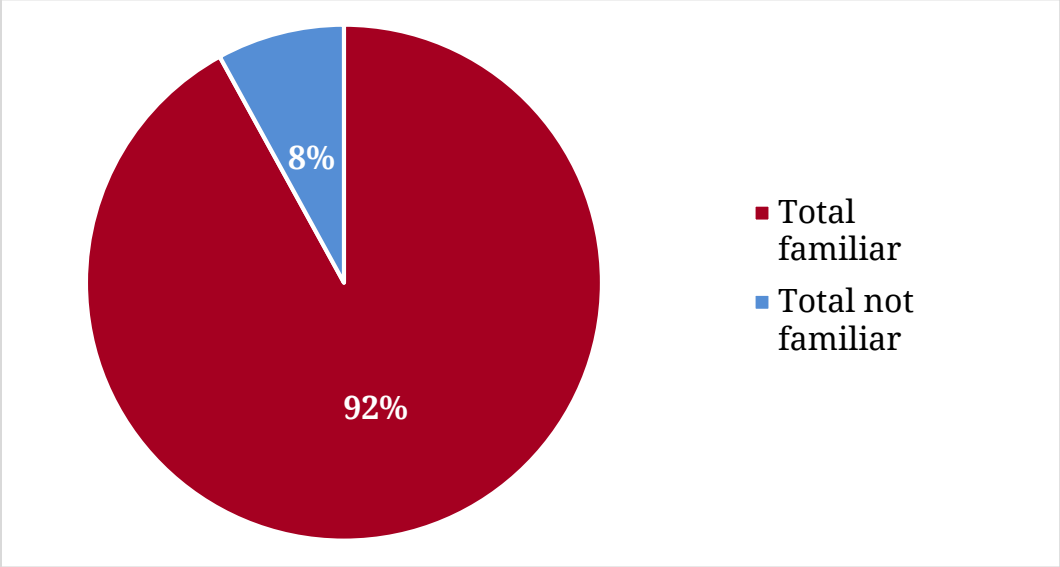
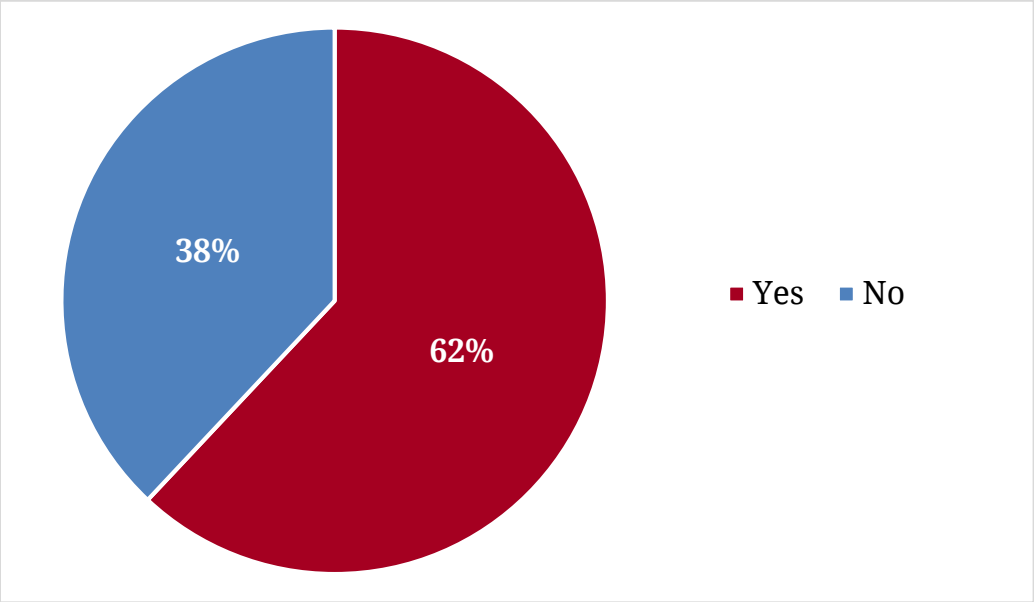
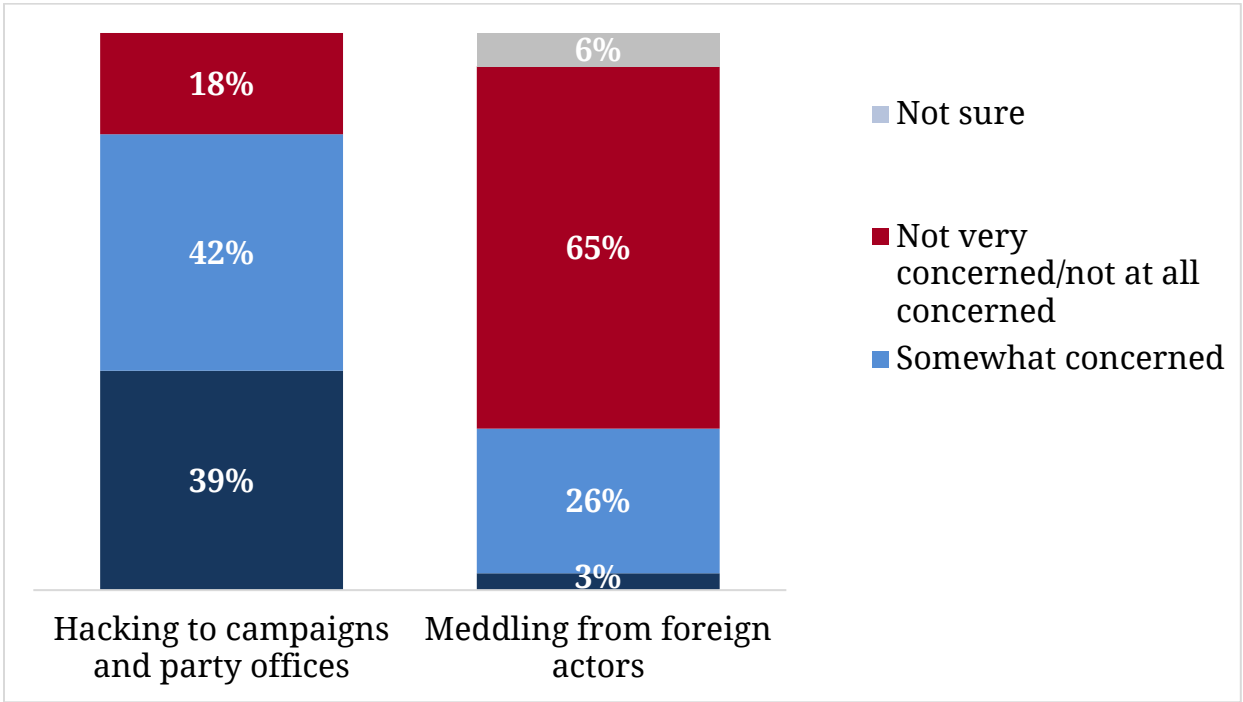


Figure 2. Aware of Spear Phishing?



The concern about hacking and interference is quite high among the campaign staffers surveyed. Indeed, 81 percent said that they are either "somewhat" or "very concerned" about stories reporting the hacking of campaigns and party offices. Fewer than 1 in 5 (18%) reported they are not concerned.

Figure 3. Concerns: Hacking and Interference



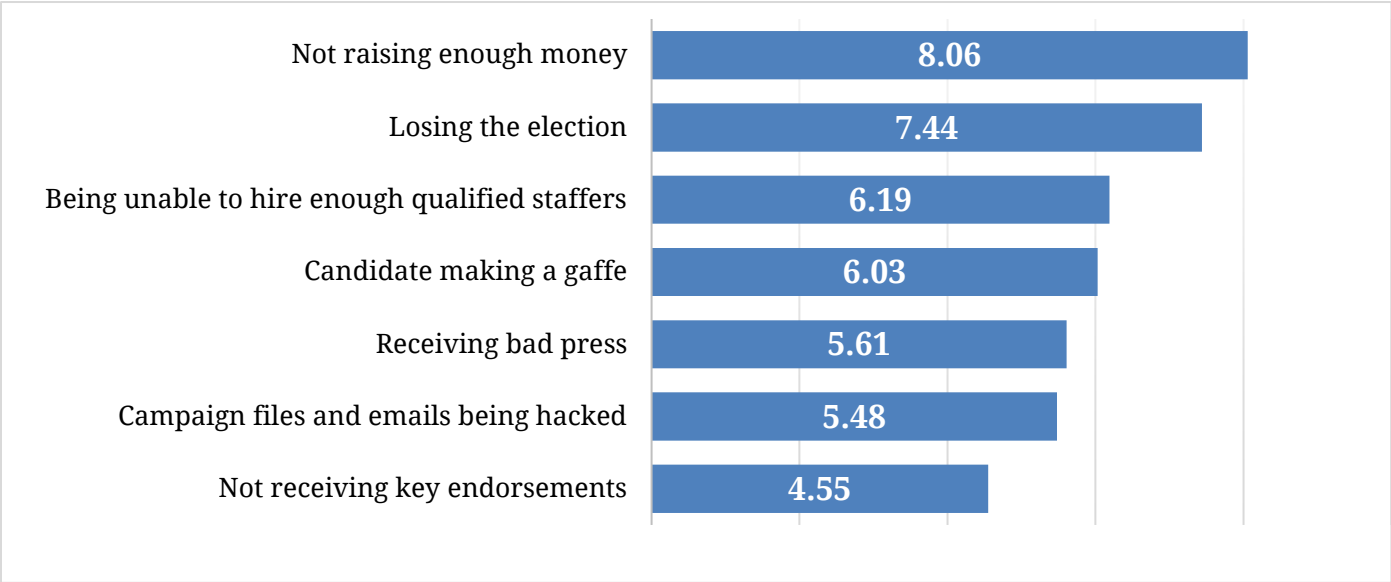
Note: Numbers may not add up to 100% due to rounding.

Nevertheless, these same campaign staffers are much less concerned about foreign actors meddling in their own campaigns. Two-thirds (65%) reported they are not "very concerned" or "not concerned at all" about foreign threats to campaign cybersecurity.

What Have Campaigns Done To Prepare For Cyber Attacks, And What Are They Willing To Do To Prevent Them?

When asked about concerns and obstacles on the campaign trail, the hacking of campaign files and emails ranked second to last, only above the risk of not receiving key endorsements. Campaign staffers are mostly concerned about losing the election or not raising enough money. Other areas of concern included an inability to hire enough qualified staffers, the candidate making a gaffe, and receiving bad press. High-level staffers generally ranked these issues as a much bigger concern to their campaigns than cyber interference.

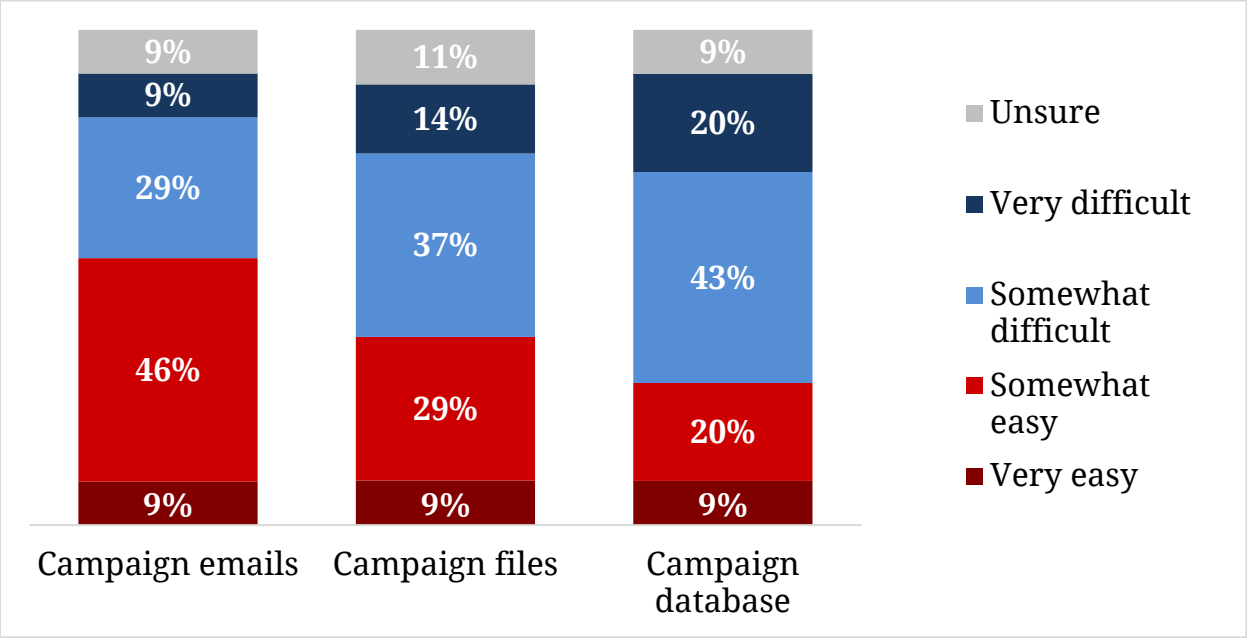
Figure 4. Campaign Concerns



Ranked on a 0 to 10 scale.

These same campaign staffers are generally confident in the security of their campaign files and databases (voter files, donor records, etc.). Half of respondents reported it would be "somewhat" (37%) or "very" (14%) difficult for someone to hack their campaign files, and even more believed it would be "somewhat" (43%) or "very" (20%) difficult for someone to hack their campaign databases. However, the campaign operatives' perspectives shifted when asked about email; half of the campaign operatives studied think it would be "somewhat" (46%) or "very" (9%) easy for someone to hack their campaign emails.

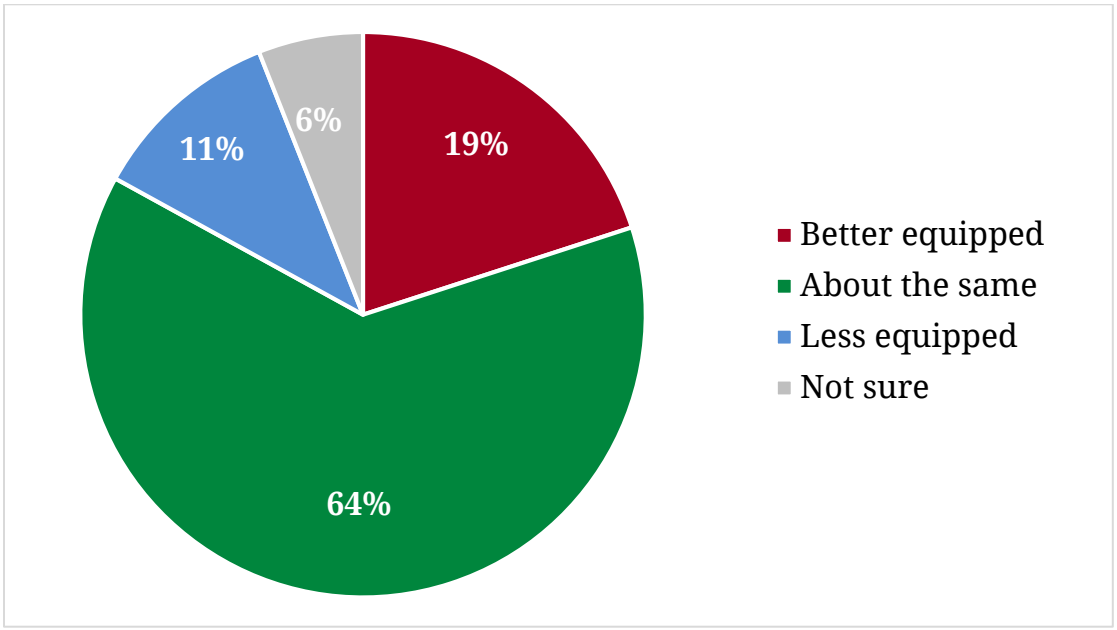
Figure 5. Difficulty to Hack



Note: Numbers may not add up to 100% due to rounding.

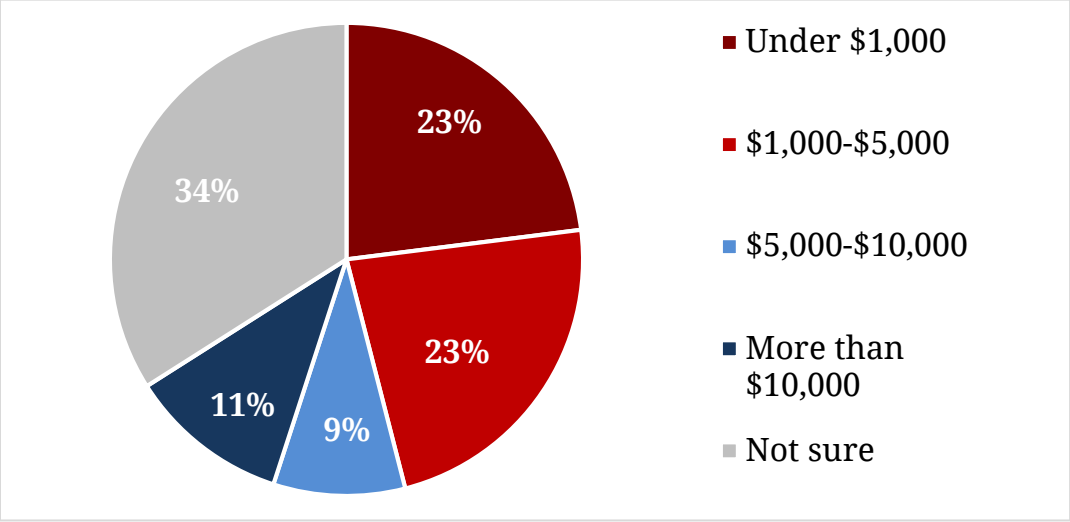
When it comes to their preparedness compared to other campaigns, staffers generally feel they are about as well-equipped as most campaigns (64%), while only 19 percent think that their current campaign is better equipped than other campaigns. Eleven percent of those surveyed believe they are less equipped compared to other campaigns and 6 percent are unsure.

Figure 6. Campaign Preparedness Compared to Others



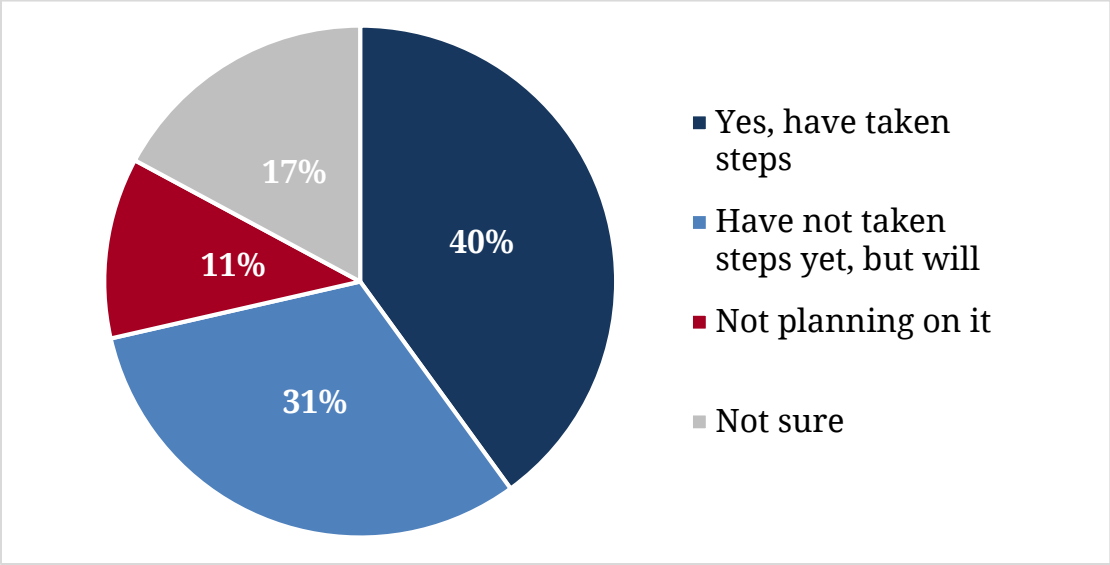
The lack of seriousness with which these staffers regard campaigns' cyber defense becomes clearer as campaigns report their willingness to spend money on added protections. Nearly half said their campaigns are willing to spend less than $5,000 on added protections against hacking, and 34 percent were not certain how much they would be willing to spend.

Figure 7. Money Willing to Spend on Cyber Protections



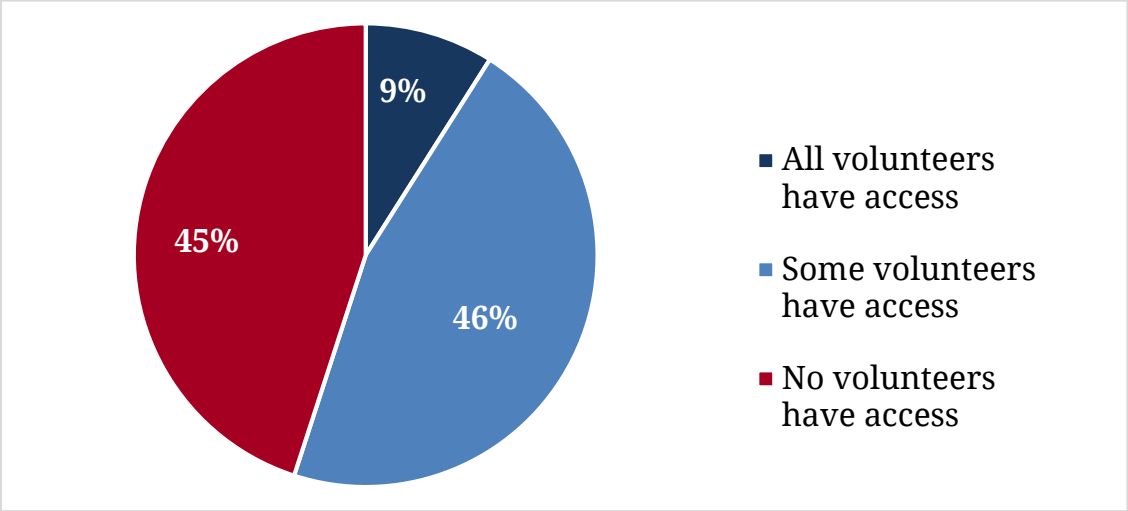
When asked whether their campaign has taken steps to prevent their network and emails from being hacked, nearly half (40%) shared they "have taken steps to protect their campaigns," while 31 percent say they have "not yet but plan on doing so in the future." Just 11 percent say they "do not plan" on taking these steps.

Figure 8. Campaign Taking Steps to Prevent Hacking



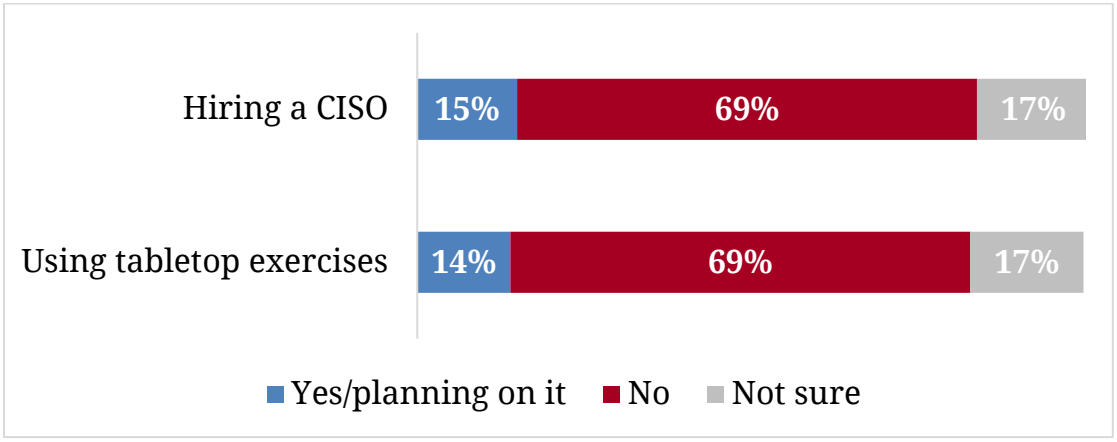
A majority of staffers surveyed have taken concrete steps toward more effective campaign security. The most common best practices include requiring passwords for staff, installing antivirus software on all campaign devices, setting up firewalls, requiring two-step verification, requiring password standards for consultants and volunteers, and not allowing campaign staff, volunteers, or consultants to use thumb drives — especially important since nearly half of campaign staffers (46%) believe that "at least" some volunteers on their campaigns have access to data.

Figure 9. Campaign Volunteers' Access to Data



Despite this, staffers are still relatively ill-prepared. The campaign operatives surveyed have not generally set up firewalls, required passwords for staff, or hired a designated staff person for information or data security. Just over two-thirds (69%) have neither hired a Chief Information Security Officer, nor an equivalent staffer. The same amount do not actively use tabletop exercises (a simulated emergency situation) to train their IT staff how to assess and respond to network vulnerabilities.

Figure 10. Protections against Hacking



Note: Numbers may not add up to 100% due to rounding.

Conclusion

While Congress completes its investigations into the 2016 presidential election, it is vital that we prepare state election officials, candidates, and their campaigns to protect themselves from cyber threats.

The White House recently announced that President Trump convened a meeting with top intelligence and legal officials to discuss the administration's plans to secure state and local election systems and to protect them from malign foreign influence. The administration's acknowledgment that election security is directly related to our national security is a critical first step in securing our elections and, more importantly, it may raise cybersecurity awareness among state and local campaigns.

The Shorenstein Center survey shows that while campaign staffs are well aware of the threat posed by cyber attacks, most are more concerned with other things, such as raising enough money or receiving bad press. They fail to recognize, as the 2016 election revealed, that a cyber attack that exposes campaign data can depress fundraising, inhibit endorsements, and create weeks of bad press.

Despite this, few campaigns have invested in cybersecurity efforts like hiring a chief information security officer or using tabletop exercises to train staff. The vital tools of modern campaigns — internet-enabled devices, software, and connectivity — need as much protection as the voting box, yet staffs and party leaders show that digital protection is not a high priority.

The threat of cyber attacks cannot be eliminated. Nevertheless, campaigns must practice vigilance and view IT and cybersecurity across the campaign organization as a necessity. Campaigns will need to adopt the necessary tools to protect against these threats and expand their budgets and staff. If not, campaigns and elections will continue to be highly vulnerable to hacking and interference.

Acknowledgments

For the second time in my political career, I was honored to return to Harvard's Kennedy School of Government. As I often tell my friends, every time the winner of the Electoral College loses the popular vote, I get to go to Harvard for a semester. Like 2000, the 2016 presidential election was one of the most disruptive campaigns in recent memory.

Special thanks to my colleagues at the Shorenstein Center on Media, Politics and Public Policy. Nicco Mele, Director of the Shorenstein Center, along with Executive Director Nancy Palmer, Communications Director Nilagia McCoy, and Professor Thomas Patterson gave insights and recommendations to look beyond the 2016 presidential election and to focus on how cyber security should be a major focus of political campaigns in the future.

I also had the assistance of Michael Auslen who helped me monitor and track congressional and statewide legislation to restore the integrity to our electoral process, along with Matthew Spector who helped draft and analyze the campaign survey.

Thank you to my bipartisan team of advisors who not only helped draft and review the final survey and results, but also helped to disseminate the survey to campaign officials. They include Stefan Hankin and Anne Hazlett of Lincoln Park Strategies, former Virginia gubernatorial candidate Ed Gillespie, the Democratic Governor's Association, the National Association of State Legislators, Celinda Lake of Lake Research Partners, Whit Ayres of North Star Opinion Research, and Neil Newhouse of Public Opinion Strategies.

Finally, I must thank the graduate students at the Kennedy School for checking in and spending time reminiscing about the election, the undergraduate students, the Institute of Politics, The Belfer Center for Science and International Affairs, and the faculty at the Kennedy School.

Appendix: A Survey of Campaign Staff

Thank you very much for taking the time to complete this survey, which covers a handful of different issues regarding the campaign you work on. Your opinions are incredibly valuable to this study and we really appreciate your time and attention.

We are planning to make the results of this survey public, but your identity and individual responses will be kept confidential and will only be shared in the aggregate.

1. Starting out, we want to make sure we're talking to a lot of different kinds of people. What is your position in the campaign?

- Campaign manager
- Finance director
- Field director
- Finance assistant
- Volunteer coordinator
- Communications director
- Digital director
- Other (please specify)
- Prefer not to say

2. And to whom do you directly report?

- Campaign manager
- Finance director
- Field director
- The candidate
- A consultant
- Other (please specify)
- Prefer not to say

3. Is this your first political campaign, or have you worked on previous campaigns?

- First campaign
- Previous experience
- Prefer not to say

4. In which state is your campaign?

5. For what elected office is the candidate running?

- Governor
- U.S. Senate
- U.S. House of Representatives

- State Senate
- State House
- Other statewide office
- Local office
- Other (please specify)
- Prefer not to say

6. What is the candidate's political party?

- Democrat
- Republican
- Green
- Libertarian
- Non-Partisan
- Other
- Prefer not to say

7. Thank you. Now, how concerned are you that each of the following may occur during your campaign? Please rate each of the following on a scale of 0 to 10, with 10 representing extreme concern and 0 representing no concern. You may use any number between 0 and 10.

- Not raising enough money
- Being unable to hire enough qualified staffers
- Receiving bad press
- Losing the election
- Campaign files, emails or databases being hacked
- Not receiving key endorsements
- Candidate making a gaffe

8. How familiar are you with the recent news focusing on hacking into political campaigns and party offices during the 2016 election cycle?

- Very familiar
- Somewhat familiar
- Not very familiar
- Not at all familiar
- Not sure

9. And on a scale from 0 to 10 where a ten means very concerned and a zero means not concerned at all, how concerned are you about these stories about hacking of campaigns and party offices? You can use any number from 0 to 10.

10. How easy do you think it would be for someone to hack into your campaign emails and/or senior campaign officials' personal email accounts?

- Very easy
- Somewhat easy
- Somewhat difficult
- Very difficult
- Not sure

11. How easy do you think it would be for someone to hack your campaign files?

- Very easy
- Somewhat easy
- Somewhat difficult
- Very difficult
- Not sure

12. How easy do you think it would be for someone to hack your campaign databases (e.g. voter files, donor records, etc.)?

- Very easy
- Somewhat easy
- Somewhat difficult
- Very difficult
- Not sure

13. And do you feel your campaign is better equipped to deal with hacking than most campaigns, about the same as most campaigns, or less equipped than most campaigns?

- Better equipped
- About the same
- Less equipped
- Not sure

14. Compared to previous campaigns you have worked on, do you believe this campaign is better prepared, not as well prepared, or about as well prepared to deal with hacking?

- Better prepared
- About the same
- Less prepared
- Not sure

15. How much money has your campaign raised?

- Less than $50,000
- $50,000 to $99,999
- $100,000 to $249,999

- $250,000 to $499,999
- $500,000 to $999,999
- More than $1 million
- Prefer not to say

16. How much is your campaign currently spending on cybersecurity protections?

- Under $1,000
- $1,000-$5,000
- $5,000-$10,000
- More than $10,000
- Not sure

17. How much is your campaign willing to spend for additional protections against hacking?

- Under $1,000
- $1,000-$5,000
- $5,000-$10,000
- More than $10,000
- Not sure

18. In general, how concerned are you about foreign actors meddling in your current race by hacking?

- Very concerned
- Somewhat concerned
- Not very concerned
- Not concerned at all
- Not sure

19. On a scale from 0 to 10 where a ten means very concerned and a zero means not concerned at all, please rate how concerned you would be about the following possible outcomes if your campaign were hacked. You can use any number from 0 to 10.

- Bad press
- Private emails disclosed
- Campaign strategy exposed
- Donor information released
- Opposition research released
- Candidate embarrassed by claim of poor cybersecurity

20. Are there any other concerns you would have if your campaign were hacked?

21. Has your campaign taken steps to prevent your network and emails from being hacked?

- Yes
- Not yet, but will
- No, not planning on it
- Not sure

22. *If answer is no, not planning on it:* What is the main reason your campaign is not planning on taking steps to prevent your network and emails from being hacked?

23. *If answer is yes or not yet:* What steps has your campaign taken to prevent your campaign from being hacked? Please mark all that apply.

- A designated staff person or full-time consultant being hired for information or data security
- Employees being trained in information security
- Requiring two-step authentication for your network
- Installing anti-virus software on all campaign devices
- Scanning your network frequently to find vulnerabilities or intrusions
- Using a strong password manager system on your network
- Encrypting all campaign devices
- Requiring minimum password standards for staff
- Requiring minimum password standards for volunteers
- Requiring minimum password standard for consultants
- Not allowing campaign staff, volunteers, or consultants to use thumb drives
- Setting up firewalls
- Using an encrypted message service such as WhatsApp or Signal

24. What other steps has your campaign taken to prevent being hacked?

25. And what is the position/title of the designated staff person the campaign hired for information or data security?

26. Does the campaign currently allow volunteers to have access to the campaign's network?

- Yes, all volunteers have access
- Yes, some volunteers have access
- No volunteers have access
- Not sure

27. What kind of log in credentials are required to access your network system?

28. Has your campaign hired a Chief Information Security Officer or equivalent role?

- Yes
- Not yet but planning on it
- No
- Not sure

29. Are you actively using tabletop exercises (a simulated emergency situation) to train your IT staff and determine network vulnerabilities?

- Yes
- No
- Not sure

30. Are you aware of what spear phishing is?

- Yes
- No
- Not sure

31. If you suspected that your data was breached, what actions would you take? Please select all that apply.

- Contact the police/FBI
- Report it to supervisor
- Report it to the candidate
- Report it to the local party head quarters
- Report it to the state party office
- Report it to the national party office
- Other-Specify
- Not sure

32. Do you have any other thoughts on this topic that you would like to share that have not been discussed in this survey?