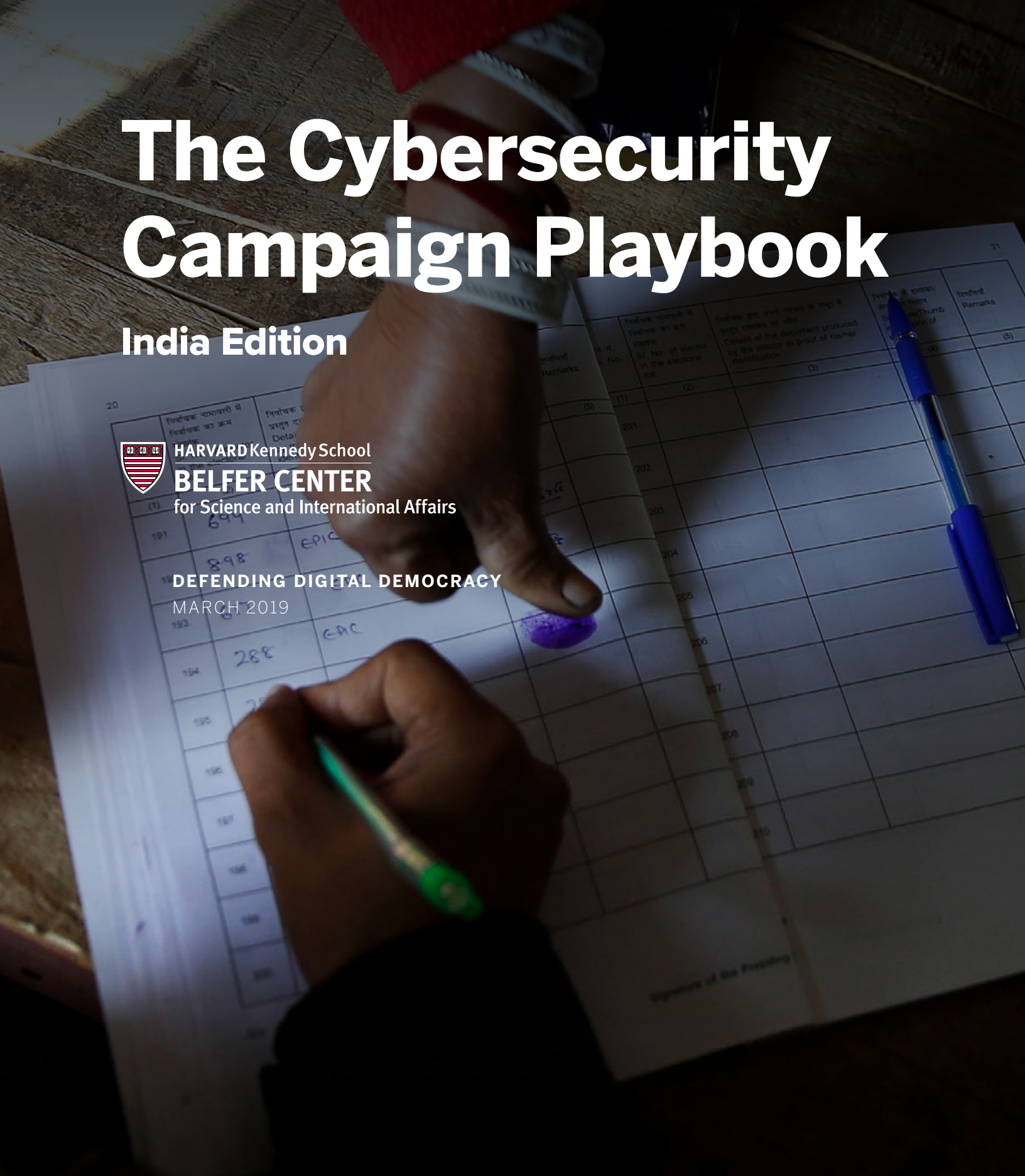
The Cybersecurity Campaign Playbook

India Edition



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY

MARCH 2019

Adapted in partnership with

NDI

IRI International Republican Institute

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/D3P

India Version partners:

The National Democratic Institute
www.ndi.org

The International Republican Institute
www.iri.org

Design & Layout by Andrew Facini

Cover photo: An indian woman puts her thumb imprint before proceeding to cast her vote, as a polling officer notes down her details at a polling station in New Delhi, India, Saturday, Feb. 7, 2015. (AP Photo/Manish Swarup)

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
MARCH 2019

The Cybersecurity Campaign Playbook

India Edition

Contents

Welcome

People join campaigns for different reasons: electing a leader they believe in, advancing an agenda, cleaning up government, or experiencing the rush and adrenaline of campaign life. These are some of the reasons we got involved in politics. We certainly didn't sign up because we wanted to become cyber experts and we're guessing you didn't either.

Unfortunately, security threats are increasing and have the power to totally upset your campaign. We come from the world of campaigns and supporting international democratic processes, and have seen first-hand the ways in which hacking, disinformation and website takedowns can affect the course of an election - and the direction of a country.

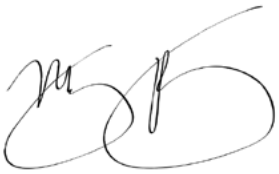
D3P is a bipartisan team of cybersecurity and policy experts from the public and private sectors, as well as experts with deep experience in political campaigns. We partnered with the International Republican Institute (IRI) and the National Democratic Institute (NDI) to better understand the Indian election landscape and how to think about and protect against digital risks.

We come from different political parties and don't agree on much when it comes to public policy, but one thing uniting us is the belief that voters should decide our elections and no one else. Our increasingly digital way of living and working offers new ways for adversaries to influence our parties, campaigns and elections. While you don't need to be a cyber expert to run a successful campaign, you do have a responsibility to protect your candidate and organization from adversaries in the digital space. That's why Defending Digital Democracy, a project of Harvard Kennedy School's Belfer Center for Science and International Affairs, created this Cybersecurity Campaign Playbook [PDF]. The National Democratic Institute, International Republican Institute and dozens of elected officials, security experts and campaign professionals worked with the Defending Digital Democracy Project to adapt this playbook for an Indian context.

The information assembled here is for any campaign in any party. It was designed to give you simple, actionable information that will make your campaign's information more secure from adversaries trying to attack your organization—and your country's democracy. Most of all, we hope this resource allows you to spend more time on what you signed up for—campaigning.

Good luck.

Robby Mook
Hillary Clinton 2016 Campaign Manager.



Matt Rhoades
Mitt Romney 2012 Campaign Manager.

P.S. Do you see a way to make the Playbook better? Are there new technologies or vulnerabilities we should address? We want your feedback. Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #CyberPlaybook or email us at connect@d3p.org, so we can continue to improve this resource as the digital environment changes

Authors and Contributors

This project was made possible by dozens of people who generously volunteered their time. Special thanks are due to **Debora Plunkett** for leading the project and **Harrison Monsky** for writing the document. We are also indebted to the people listed below who invested countless hours in reviewing drafts and providing input.

Special thanks to **Jan Neutze**, Managing Director, Microsoft Defending Democracy Program and team for funding the development of the India edition of the Playbook

DEFENDING DIGITAL DEMOCRACY LEADERSHIP

Eric Rosenbach, Co-Director, Belfer Center

Robby Mook, Belfer Center Fellow

Matt Rhoades, Belfer Center Fellow

AUTHORS AND CONTRIBUTORS

Heather Adkins, Director, Information Security and Privacy, Google

Dmitri Alperovitch, Co-founder and CTO, CrowdStrike

Ryan Borkenhagen, IT Director, Democratic Senatorial Campaign Committee

Josh Burek, Director of Global Communications and Strategy, Belfer Center

Michael Chenderlin, Chief Digital Officer, Definers Public Affairs

Robert Cohen, Cyber Threat Analyst, K2 Intelligence

Chris Collins, Co-Founder, First Atlantic Capital

Caitlin Conley, D3P, Harvard Kennedy School

Julia Cotrone, Special Assistant, Definers Public Affairs

Jordan D'Amato, D3P, Harvard Kennedy School

Mari Dugas, Project Coordinator, D3P, Harvard Kennedy School

Josh Feinblum, D3P, Massachusetts Institute of Technology

John Flynn, Chief Information Security Officer, Uber

Siobhan Gorman, Director, Brunswick Group

Daniel Griggs, Founder and CEO, cmdSecurity Inc.

Stuart Holliday, CEO, Meridian International Center

Eben Kaplan, Principal Consultant, CrowdStrike

Greg Kesner, Principal, GDK Consulting

Kent Lucken, Managing Director, Citibank

Katherine Mansted, D3P, Harvard Kennedy School

Ryan McGeehan, Member, R10N Security

Jude Meche, Chief Technology Officer, Democratic Senatorial Campaign Committee

Nicco Mele, Director, Shorenstein Center

Eric Metzger, Founding Partner and Managing Director, cmdSecurity Inc.

Zac Moffatt, CEO, Targeted Victory

Harrison Monsky, D3P, Harvard Law School

Debora Plunkett, Former Director of Information Assurance, National Security Agency

Colin Reed, Senior Vice President, Definers Public Affairs

Jim Routh, Chief Security Officer, Aetna

Suzanne E. Spaulding, Senior Adviser for Homeland Security, Center for Strategic and International Studies

Matthew Spector, D3P, Harvard Kennedy School

Irene Solaiman, D3P, Harvard Kennedy School

Jeff Stambolsky, Security Response Analyst, CrowdStrike

Alex Stamos, Chief Security Officer, Facebook

Phil Venables, Partner and Chief Operational Risk Officer, Goldman Sachs

Frank White, Independent Communications Consultant

Sally White, D3P, Harvard University

Rob Witoff, Senior Security Manager, Google

Contributors from the **National Democratic Institute** and the **International Republican Institute**

BELFER CENTER WEB & DESIGN TEAM

Andrew Facini, Publications and Design Coordinator, Belfer Center

The Playbook Approach

This Indian Cybersecurity Campaign Playbook was written by a multi-partisan and international team of experts in cybersecurity, politics, and law to provide simple, actionable ways of countering the growing cyber threat.

Cyber adversaries don't discriminate. Campaigns at all levels – not just high-profile national campaigns – have been hacked. You should assume you are a target. While the recommendations in this playbook apply universally, it is primarily intended for parties and campaigns that don't have the resources to hire professional cybersecurity staff. We offer basic building blocks of a cybersecurity risk mitigation strategy that people without technical training can implement (although we include some things which will require the help of an IT professional).

These are baseline recommendations, not a comprehensive reference to achieve the highest level of security possible. We encourage all parties and campaigns to enlist professional input from credentialed IT and cybersecurity professionals whenever possible.

Introduction

Campaigns and political parties increasingly rely on the internet, digital technologies, and social media to reach and engage with potential voters and to develop campaign messaging and strategy. In the United States, savvy use of data analytics and social media were critical to the victories of both former President Barack Obama and President Donald Trump. Much like Obama's 2008 campaign, 2014 marked a turning point in Indian campaigning. In those general elections, Prime Minister Narendra Modi and the Bharatiya Janata Party (BJP) used a number of innovative and unique digital approaches to gain advantage, including crowdsourcing speech topics online, broadcasting simultaneous rallies using 3D holographic technology, and organizing effective cross-platform social media campaigns. Many of these unique approaches are now mainstreamed across Indian campaigns from the national to local level within parties large and small.

Candidates and campaigns face a daunting array of challenges. There are events to organize, volunteers to recruit, public rallies to manage, funds to raise, voters to contact, and the relentless

demands of the modern media cycle. Every staffer must anticipate unfortunate surprises like gaffes or a last-minute attack ad. While the internet and digital technology have made some of these challenges easier to manage, the digitization of campaigns and parties presents adversaries with new opportunities to meddle, disrupt, steal and otherwise negatively affect campaigns.

Cyber attacks, misinformation campaigns, data breaches and internet censorship now belong on the list of common campaign challenges. In 2008, Chinese hackers infiltrated the Obama and McCain campaigns in the US, and stole large quantities of information from both. In 2016, cyber operatives believed to be sponsored by the Russian government stole and leaked tens of thousands of emails and documents from US Democratic Party campaign staff, feeding disruptive disinformation campaigns. In 2017, Kenyan political parties faced widespread disinformation campaigns online. More recently, in January 2019, hundreds of German politicians including Chancellor Angela Merkel were targeted by hackers, who published personal details and communications on social media sites.

India is no stranger to these types of cyber attacks and disinformation campaigns. In November 2016, the Twitter handle of Indian National Congress President Rahul Gandhi appeared to have been co-opted by hackers and sent out a series of abusive tweets. In April 2018, India's Ministry of Defence website was hacked, with the homepage replaced with a Mandarin character, fueling speculation that the attack was conducted by Chinese hackers. And, on a much more tragic level, the summer of 2018 underscored how targeted misinformation and rumors spread via messaging apps and social media platforms can harm healthy political discourse, inflame social tensions, and even lead to violence.

Indian parties and campaigns should expect and plan for these types of incidents to occur more frequently and at a wider scale.

Cybersecurity breaches can derail a candidate's message for months by diverting media attention away from policy proposals, through slow-drip releases of stolen information, or by hijacking campaign websites and social media accounts. Co-opted social media accounts can be weaponized by maligned actors to sow political confusion and discord and elevate misinformation campaigns. Attackers overloading a website can cut off communications to your supporters or lead to lost donations at key moments. The theft of personal donor or voter data can generate significant legal liabilities, open supporters to harassment, and make donors reluctant to contribute to a campaign. Destructive attacks aimed at staff computers or critical campaign servers can slow down

campaign operations for days or even weeks. Cleaning up the resulting mess will divert precious resources in the heat of a close race, whether it's for prime minister, MP, MLA or local council.

For the foreseeable future, cyber threats will remain a real part of our campaign process. Ironically, one of the most celebrated aspects of Indian democracy – its diversity and sheer size – means that its democratic institutions must be hyper-vigilant. India is home to more than 1.3 billion people, representing numerous religions, ethnicities, and linguistic groups. More than 1,800 political parties are registered at the local, state, and national levels with the Election Commission of India. State-level elections in India frequently involve more voters than the national elections of most countries. Many of the country's political institutions, including political parties, must operate in a decentralized manner to accommodate the scale and diversity of Indian democracy. While this arrangement allows for elections and political campaigns to take place on a scale that is unprecedented elsewhere in the world, it also means that defending Indian democracy will require all political parties and campaigns – even at the local and state level - to prioritize cyber defense and contingency planning.

As democracy's front line, party and campaign staff must recognize the risk of an attack, develop a strategy to reduce that risk as much as possible, and implement response strategies for that moment when the worst happens. While no campaign can achieve perfect security, taking a few simple steps can make it much harder for malicious actors to do harm. The most sophisticated state actors often choose the least sophisticated methods of attack, preying on people and organizations who neglect basic security protocols. That is our primary reason for creating this Indian editionof the Cybersecurity Campaign Playbook.

In today's campaigns, cybersecurity is everyone's responsibility. Human error or confusion is consistently at the root of cyber attacks, and it's up to the candidate and campaign leaders to weave security awareness into the culture of the organization. The decisions humans make are just as important as the software they use. Going forward, the best campaigns will have clear standards for hard work, staying on message, being loyal to the team—and following good security protocol.

Before we get into our recommendations, let's quickly frame the problem:

- **the environment in which your campaign is operating;**
- **the threats your campaign will likely face; and,**
- **the importance of cyber risk management**

The Vulnerable Campaign Environment

Today's campaigns are uniquely soft targets. They're often inherently temporary and transient. They don't have the time or money to develop long-term, well-tested security strategies. Large numbers of new staff and volunteers are often on-boarded quickly without much time for training. They may bring their own hardware from home – and the malware lurking on it! Given the decentralized nature of parties and campaigns in India, many contributors live and work hundreds of kilometers away from the headquarters. Things move fast, the stakes are often high, and people feel like they don't have the time to care about cybersecurity. There are a lot of opportunities for something to go wrong.

At the same time, parties rely more and more on proprietary information about voters, donors, and public opinion. They also store sensitive documents like opposition research, vulnerability studies, supporter lists, personnel vetting documents, first-draft policy papers, and emails. The risks of a potential attack are increasing and so are the consequences.

THE DANGER OF AN ATTACK

Picture this: It's a month before Election Day, and the race is tight. You arrive at headquarters early, get some coffee or tea, get to your desk, and log into your computer. A black screen pops up, then a gruesome cartoon of your candidate, followed by a message. Your hard drives have been wiped clean. Every digital bit of information you've gathered—memos, targeting lists, balance sheets—is gone. Getting it back, you read, will cost a fortune - or the renunciation of a major policy position.

An unidentified group hacked into your computer months ago, and has been quietly stealing emails, strategy memos, donors' addresses, and staffers' national ID numbers. The group has spent weeks combing through the bounty in search of dirty laundry and has been distributing the highlights on social media, using some of it to fuel misinformation against the campaign and candidates For now, the campaign's website is down, its social media accounts and direct messaging channels have been suspended for pushing out lewd images, and there's not a working computer in sight.

The Threats Campaigns Face

Unfortunately for campaigns and democracies around the world, domestic and foreign adversaries may think that harming or helping a particular candidate advances their interests, whether that means creating chaos and confusion among voters, or punishing an official who has spoken out against them. This may sound like thriller fiction, but the reality is that a sophisticated intelligence service, cybercriminal or hacktivist with a grudge against a candidate, could decide that you or someone on your campaign is a target. These are the sorts of threats leaders and staffers have to realize are possible. With a growing number of publicized efforts to tamper with elections electronically, the public will also be quick to assume an incident is related to a cybersecurity problem--even when it is not.

As disinformation and manipulated campaign communications become a source for deceiving and misleading citizens around the world, stolen, manipulated and leaked information can lead to real consequences in your election. The mechanisms that you have in place for protecting your data and maintaining communication channels are more important than ever before.

WHO'S HACKING?

Parties and campaigns face information and cybersecurity threats from a wide array of actors. Lone “black hat” hackers and cybercriminals have tried compromising campaigns for reasons of personal gain, notoriety, or the simple desire to see if they could. Nation-states pose the most dedicated and persistent threat. Russian espionage groups known as “Fancy Bear” (APT 28) and “Cozy Bear” (APT 29) were implicated in the 2016 campaign hacks in the US. The Chinese have focused much more on information gathering. They are believed to have been active in the 2008 and 2012 US presidential campaigns, but there is no evidence they released any stolen materials. The North Koreans infamously retaliated against Sony Pictures Entertainment for producing the film, *The Interview*, by stealing and releasing company emails and wiping their systems. Competing domestic campaigns can also pose cybersecurity threats to each other. Heightened international tensions - particularly around high-stakes elections - could prompt more attacks in the future as well.

Managing Cyber Risk

Risk is best understood in three parts. First, there are *vulnerabilities*: weaknesses in your campaign that make information susceptible to theft, alteration, or destruction. Vulnerabilities can originate in hardware, software, processes, and in the vigilance level of your staff and volunteers. Then there are actual *threats*: the nation-states, competing campaigns, hacktivists, and other nonstate groups with the capability to exploit those vulnerabilities. Risk exists where vulnerabilities and threats meet. Lastly, there are consequences--the impact when malicious actors capitalize on unmitigated risk.

There's nothing you or your campaign can do to prevent threats themselves – they are the result of larger political, economic, and social forces. What you can do is substantially reduce the likelihood that your adversaries will succeed by reducing how vulnerable you are. Reducing vulnerability reduces risk – it's up to you to decide which ones are most essential to reduce. For example, you may decide that the most damaging thing a hacker could do is to steal your party or candidate's self research report, so you will devote extra resources for secure data storage, require long account passwords and restrict access to a small number of people. You may decide to make other documents within the party and campaign more widely available and less secure, since more people need them to do their job and they wouldn't cause much damage if they were leaked. Note that the steps that campaigns take to secure their data and respond to any cyber incidents are also subject to the same data protection and privacy laws that govern other types of personal information in India..

There are technical aspects to risk mitigation and we have many technical recommendations in this playbook, but what matters most is your holistic approach. As a party and campaign leader, the most important thing you can do is make fundamental choices, such as who has access to information, what information is kept or discarded, how much time you devote to training, and your own behavior as a role model. As a campaign leader, risk management is your responsibility – both technical and human. It's up to you to decide what data and systems are most valuable and what resources you commit to protect it.

Securing Your Campaign

Our security recommendations are organized according to three principles:

1. Prepare:

The success of nearly every one of the Playbook's recommendations depends on leadership creating a culture of security vigilance that minimizes weak links across the party and campaign structure. That means establishing clear ground rules that are enforced at the national, state and local level from the top down and are embraced from the bottom up.

2. Protect:

Protection is critical. When you discover you have a security problem, it is already too late. Building the strongest defenses that time and money allow is key to reducing risk. Internet and information security works best in layers: there is no single, bulletproof technology, strategy, behavior or product. A few basic measures used in combination can make a campaign's digital architecture more difficult to breach and more resilient if compromised, ultimately saving your campaign time and money in the future.

3. Persist:

Campaigns now face adversaries with ever-increasing levels of resources and expertise; even the most vigilant culture and the toughest infrastructure may not prevent a security breach. Parties and campaigns need to develop a plan ahead of time to deal with a breach if one occurs.

Some campaigns have more time and money for cybersecurity than others. That's why our recommendations offer two tiers of protection: "good" and "enhanced." The "good" tier represents everything a party and campaign must do to have a minimum level of security. You should always aspire to do more as time, money, and people allow, which is why we recommend using the "enhanced" level whenever possible. If you have the resources to get reputable, trained IT support, it's money well spent. Threats are constantly evolving and professional IT services will help get you beyond what this playbook provides and keep you abreast of the latest threats and solutions for your situation.

Leadership

Campaign and party leadership need to take responsibility for their cybersecurity strategy, but most will delegate development and supervision to a technology or operations point-person. It's important that cybersecurity is tightly integrated into all elements of a party and campaign, especially staff and volunteer recruiting (human resources) and information technology, communications and outreach work, since correctly onboarding staff and volunteers, provisioning hardware, and controlling accounts, systems and permissions will be critical to your strategy. For volunteers in particular, it is key to thoroughly vet them and carefully control access, so that volunteer support doesn't create new vulnerabilities. You should make sure that full-time party and campaign staff are supervising IT work and controlling permission to access different systems up and down the party structure.

When To Start

Whatever support model you have, *cybersecurity should start on Day One*. What follows is a "top five checklist" of measures that are absolutely vital. Make sure these are in place at the very beginning, then complete the other "good" recommendations as soon as possible. If these measures were not part of your first digital plan, don't worry. It isn't too late to adopt effective security measures and protect what you are already doing.

Cost

A lot of what we recommend here is free or very low cost. In fact, everything on our top five list is free. High target campaigns will need to budget enough resources for hardware and software to execute a responsible strategy, but this should still be a very small percentage of a campaign budget. Smaller campaigns will be able to execute the recommendations here for a few hundred to a few thousand dollars depending on how many staff or volunteers work on the campaign.

Any references to vendors and products are intended to help provide examples of common solutions, but do not constitute endorsements. If challenges arise when implementing products or services, we encourage you to reach out directly to the vendors, who can usually provide user-level technical assistance. When it comes to product and service selection, we encourage every campaign to consult with a cybersecurity expert or conduct independent research to find the best product for their needs.

Top Five Checklist

1. Establish a culture of information security awareness:

Take cybersecurity seriously. Take responsibility for reducing risk, train your staff and volunteers, and set the example. Human error is the number one cause of breaches.

2. Protect your devices:

Keep all devices - smartphones, computers, tablets - well protected. Your devices should be locked with a strong passcode or passphrase, kept physically secured, and operating systems should be updated regularly. A poorly secured device makes it easier for your adversaries to steal and leak sensitive information and to access or take over many of your most important accounts (like social media profiles).

3. Use two-factor authentication (2FA) and strong passwords:

Require two-factor authentication (2FA) in order to add a second layer of protection for all important accounts, including your office suite, any other email or storage services, and your social media accounts. Use a mobile app or physical key for your second factor, not SMS text messaging. For your passwords, create SOMETHINGREALLYLONGLIKETHISSTRING, not something really short like Th1$. Contrary to popular belief, a long string of random words without symbols is more difficult to break than something short, with L0t$ 0f $ymB01$. Never repeat passwords; a password manager can help with this too, by allowing you to randomly generate strong passwords and audit your existing passwords to identify ones that have been reused.

4. Use encrypted messaging for sensitive conversations and materials:

Using an encrypted messaging tool for phones like Signal for sensitive messages and documents means adversaries can't get them if they hack into your email. Encryption scrambles the data, dramatically reducing the likelihood that someone can read your messages, even if they intercept the data.

5. Plan and prepare:

Have a plan in case your security is compromised. Know whom to call for technical help, understand your legal obligations, and be ready to communicate internally and externally as rapidly and effectively as possible.

Steps to Securing Your Campaign

Step 1: The Human Element

Cybersecurity is fundamentally a human problem, not a technical one. The best technical solutions in the world will have no effect if they are not implemented properly, or if they are not continuously updated as technology evolves. Successful cybersecurity practices depend upon creating a culture of security.

GOOD — What You Need to Do

1. Establish a strong information security culture that emphasizes security as a standard for a winning campaign. Staffers and volunteers should know to avoid clicking on links or opening attachments in emails from unknown senders.

    a. **Onboarding**: Provide basic information security training when you onboard new staff and volunteers. You can distribute the Staff Handout at your training.

    b. **Trainings**: Make security part of all your ongoing staff trainings, such as senior staff events or pre-election get-out-the-vote (GOTV) trainings. Provide additional training for those in sensitive roles, such as candidates, media and communications staff, high-profile staff, and anyone with system administrator privileges on your network. Leadership should require that the most important people in the party and campaign—including the candidates—have their security settings checked by whoever runs IT (that may be the manager herself). Don't be timid or half-hearted about security for candidates and other VIPs!

    c. **Set the example**: Senior staff and candidates must take a visible leadership role, advocating for cybersecurity during trainings. Leadership should provide periodic reinforcement of cybersecurity's importance to others in meetings and on calls. Don't just have technical experts conduct trainings. The campaign lead or operations director can be a more powerful messenger precisely because they're seen as less "technical."

2. Conduct a thorough vetting of staff and volunteers—anyone requesting access to party and campaign information—to avoid giving credentials to someone who wants to steal data or sabotage your systems.

    a. Establish a definition for sensitive information and rules for its use. For example, you could choose to classify all polls, research materials, strategy memos, and related emails as "sensitive."

b. Prohibit the transfer of sensitive information on communication channels that aren't managed and secured by the campaign. You can require that it be transferred only through encrypted messaging (see Step 2).

3. Confirm that consultants and vendors with access to sensitive information have secure email and storage (see Step 2). When in doubt, require vendors and consultants to use an account on your cloud-based office suite (See Step 2).

4. Control access to important online services, such as the official party and campaign social media accounts, to prevent use by unauthorized individuals. Make sure that those who leave the party or campaign can no longer access campaign-related accounts. You can do this easily by using a social media account management tool that acts as a gateway to all your accounts. If someone leaves the campaign, you should immediately disable their account.

5. Educate staffers about the phishing threat. Make sure they know how to spot and avoid suspicious links and emphasize the importance of identifying and reporting potential phishing attacks. As part of the party and campaign's strong security culture, leadership should recognize and praise anyone who reports suspicious behavior on their system or admits to clicking a potentially malicious link.

6. Understand your legal environment. Current and proposed legislation may mandate particular requirements for any data your party and campaign may collect, particularly personally identifiable information like demographic or address data.

Handouts

» For Staff

» For Family Members

ENHANCED — Take the Next Step

1. Software products such as Phishme and KnowBe4 can train your staff by sending them fake phishing emails. This is a safe, quick, and effective way to learn who is at risk of clicking a link, so you can give them extra training. Many of these products also filter some phishing attempts out of your email.

2. If you have the resources, hire a dedicated IT professional to manage your party and campaign systems and an IT security expert to help protect, maintain, and monitor your digital infrastructure. He or she can provide regular security training and testing of your people and systems, while customizing security solutions.

3. Contract with a cybersecurity firm to provide security solutions, review your defenses, and/or monitor your systems for a breach. Know which firm you want to contact if you are breached and need urgent incident response support. This is an alternative to hiring a full-time IT security expert. Do your research and go with a highly reputable firm—not all cybersecurity firms provide the same level or type of service. Just like with other external vendors, trust and communication are essential.

WORKING WITH SECURITY PROFESSIONALS

If you decide to work with a security professional, how will you evaluate the right person or firm? Whether it's through personal recommendations or positive public reviews, it's important that you avoid costly yet ineffective support. When interviewing potential security professionals, ask about how they've responded to past security incidents and how they've enabled others to work more securely. Your respective national party committee or trusted campaign professionals may be able to recommend options to choose from. Bear in mind that culture affects security and that even the best recommendations may fail to achieve results if they are not followed (i.e., just hiring a firm won't solve your problems).

Step 2: Communication

Not all methods of communication are equally secure, so be deliberate about how you communicate. Party and campaign leadership should set a standard that encourages in-person conversations whenever possible, and discourages needless or superfluous emails. Anything you write in email could be published in the newspaper or leaked on social media - perhaps after malicious modification. Whether it is phone calls, texting, or emailing, different products and services offer different levels of protection, so do your research before you choose which systems your campaign is going to use.

GOOD — What You Need to Do

1. Use the most secure systems possible for communication.
    a. Use end-to-end encrypted messaging services such as Signal, especially for messages, document sharing and phone calls. Many campaigns require that sensitive information only be transmitted by encrypted messaging, and it's often easiest for staff to get in the habit of using these apps for all routine communications (this is especially smart for high-risk individuals like candidates). Signal publishes its source code for review and provides functionality that reduces risk, such as allowing you to auto-delete messages. Be sure that your messages are not syncing to your computer or unencrypted cloud accounts.
    b. Switch off archiving or backup for messaging services, such as Google Chat, so that old chats can't be stolen later. This requires going into "settings" and adjusting "retention policy" timelines. Some services require you to do this for every single chat conversation. We recommend retaining chat messages for one week or less.

2. Use a cloud-based office suite that provides secure email communication, document creation, chat, and file sharing, such as GSuite or Microsoft365. For example, GSuite includes Google Drive for file sharing, Gmail for email hosting, Google Hangouts for chat, and Google Docs for word processing, spreadsheets, and presentations. Microsoft365 offers OneDrive/SharePoint for file sharing, Outlook/Exchange for email, Microsoft Teams for chat, and Microsoft Office for word processing, spreadsheets, and presentations. Unless you are hiring highly-experienced (and potentially costly) security professionals, cloud-based systems managed by major firms will be better protected than any servers you could set up in your party or campaign. There are free versions of both products, but the paid versions give you many more administrative capabilities. Google also offers free services to protect organizations in threatening environments such as Outline, a self-hosted VPN; Project Shield, a service to protect your website against disabling attacks; and Password Alert, which warns you if you enter your Gmail password in a phishing site.

3. Delete your email

    a. Turn on Auto-delete in your email application for old emails to reduce the number of emails that could potentially be stolen. This usually requires going in and changing "retention policy" to shorter time periods in "settings." To ensure emails do not just sit in a "deleted items" folder, adjust settings to auto purge "deleted items" folder after a certain time period. We recommend retaining emails for one month or less, unless legally required to retain them for longer periods. What you don't have can't be stolen.

4. Secure personal accounts

    a. Party and campaign business should never go on personal accounts. However, adversaries will target personal accounts, so have your staff and volunteers use strong passwords and two-factor for their personal accounts as well (this is included in our Staff Handout).

WHAT IS THE CLOUD?

"Cloud services" provide management and access to information stored remotely on the internet. They run on off-site servers managed by third-party companies; this includes many common services you may already use, such as Gmail or Dropbox. It's good to store information with a trusted cloud service provider instead of on your personal computer because these providers have the money, technical resources and expertise to make their servers more secure than your laptop's hard drive, or an office server. They also have lots of technical staff working to defend against sophisticated attacks on their networks (and therefore on your data as well). It's like the difference between leaving cash under your mattress and storing it in a bank's security vault. Using cloud services offers an additional backstop against data loss if an individual device is lost or compromised. Cloud storage is a feature included in comprehensive office security services such as GSuite and Microsoft365. Other services include Dropbox or Box. It's important to keep in mind that these international corporations may be subject to law enforcement demands for a history of contacts, emails, or contents of files. Most major corporations, including any named here, have strict policies of when they will comply with such demands.

WHAT IF I DON'T TRUST THE CLOUD?

Some organizations are uncomfortable with the idea trusting a third party company with their information. If you insist on managing your own technology infrastructure, be aware you may have to defend against the security forces of nation-states. Some considerations:

- You will be responsible for understanding, securing and patching all aspects of your systems, including operating systems, server applications, the actual software, applications, databases, and connection technologies.
- You will have to make sure the connection to your key platforms is highly reliable, and not vulnerable to manipulation, censorship or DDOS.
- You will need to actively monitor for hacks and have someone on call 24/7.
- You will need to manage secure, off-site backups.

WHAT IS ENCRYPTION?

Encryption is a way of encoding information when it travels between users, or when it's stored, so it can't be read by anyone but the intended recipient. Think of it this way: a user "scrambles" the data when she sends it and only the intended recipient has the key to unscramble it. Using encryption is smart, especially for sensitive information, because even if an adversary steals the data, it's unlikely they'll be able to read it. Most apps that use encryption, like Signal, make the process seamless. End-to-end encryption is an important feature in communications programs - it means your message is secret from your phone or computer all the way to your destination, and no one - including the app provider itself- can read the messages. If possible use whole-disk encryption on your laptop as well; if it is stolen or left on a bus, no one can read the contents.

INTERNET RESTRICTIONS AND SHUTDOWNS

Restrictions on the accessibility of the internet and blocking of critical communications channels such as, for example, WhatsApp or Twitter are becoming increasingly common. In the worst situations, access to the entire internet may be cut off.

Given this volatility, always have a backup plan. If your party or campaign is particularly dependent on your website, make sure your Facebook page has the most important information in case your website is blocked. If WhatsApp is a core communication channel, be prepared to use SMS or have a backup phone tree with everyone's numbers to stay in contact.

KEEPING YOUR WEBSITES ONLINE

Your campaign's web site is probably one of your most important public communication platforms, and one of the easiest ways for citizens to find you. This makes your online presence a particularly compelling target for malicious hackers or unscrupulous rivals. Consider using a managed hosting platform such as Wordpress.com, Wix, or Google Pages where you are not responsible for being the security administrator for a web site. If you wish to manage your own website, be sure you are yourself an expert or that you are able to hire professionals to keep it safe from hackers.

Increasingly, attackers are turning to "distributed denial of service" (DDOS) attacks to knock a site offline during critical periods through huge volumes of bogus requests. Content Distribution Networks (CDNs) are able to maintain a cached copy of your site on powerful servers all around the world, making it almost impossible to take them all down. Two products with the ability to assist by protecting the your public web sites are Cloudflare and Google's Project Shield.

Step 3: Account Access and Management

One of the most challenging aspects of security is keeping unauthorized people out. This means preventing adversaries from gaining access to your data and preventing people within your party and campaign from having access to information they do not need. While some of the recommendations below may seem cumbersome, hackers depend on those who value convenience over security.

WHAT IS TWO-FACTOR AUTHENTICATION?

Two-factor authentication is a second layer of security that requires a user to provide an extra credential beyond her or his password. The second factor is critical because, if your password is stolen, an adversary still can't log into your account. Your password is something you know and your second factor is something you have, like a code that's generated by an app, a physical key, or even something biometric, like a fingerprint.

GOOD — What You Need to Do

1. Require two-factor authentication (2FA) on all systems and applications. Avoid texting (SMS) for two-factor authentication, because attackers can easily clone a phone number and get access to texts. There are several 2FA apps that work just as easily as texting and are more secure, such as Google Authenticator, Microsoft Authenticator, and Duo Mobile. You can also use a physical FIDO ("fast identity online") key that is inserted into your USB drive such as Yubikey or Feitian. The website "TwoFactorAuth.org" is a helpful guide to services that do and do not offer 2FA.
2. Passwords.
    a. Require strong passwords. As we noted earlier, "make passwords that are long and strong." Current computing capabilities can crack a seven-character password in milliseconds. A 20-, or even 30-character password will take much longer for a hacker to crack. Choose a string of words that you can easily remember.
    b. Don't repeat passwords! Use a different password for different accounts so a hacker can't break into multiple accounts if a single password is stolen.

c. To protect party and campaign staff and volunteers against phishing attacks, only share passwords in person or over short-lived encrypted messages. Require password resets for central accounts to be requested through these same methods or over a video chat to ensure it is the actual staff member or volunteer. Never share passwords over email or store/distribute using a helpdesk system.

3. Use a password manager such as LastPass, 1Password, or Dashlane to help you manage a lot of long, strong passwords easily. But ensure that your management system has a long, strong password and two-factor authentication. We don't currently recommend password managers built into browsers such as Chrome, Safari and Firefox, which are often less secure than these standalone managers.

4. Create separate accounts for administrators and users, and severely restrict access to administrator accounts. Administrators should also have two separate campaign accounts—one used only for their admin duties and one that is their standard user account for all other party and campaign business. This will reduce the likelihood that an adversary will be able to compromise an administrator account, which would provide access to the entire network.

5. Conduct periodic reviews of who has access to different devices and networks. Immediately block access of people who leave the party or campaign. Immediately change passwords if suspicious activity is observed. To make this possible, make sure that your staff are not sharing user accounts.

PASSWORD MANAGERS

Password managers are a way to store, retrieve, and generate passwords. Some even have the ability to auto-populate the password line on login pages. The password manager requires a password of its own to login, which becomes the one password you do have to remember. The risk, of course, is that if someone breaks into your password manager (it has happened), that person will have all of your passwords. But this risk is almost always far outweighed by the benefit of strong, unique passwords across all of your accounts, and can be significantly reduced by using two-factor authentication on your password manager. For campaigns, password managers sometimes make sense for accounts that have multiple users, because the administrator can safely share access to them.

ENHANCED — Take the Next Step

1. Create user profiles for different types of party and campaign staff that automatically grant the necessary level of access. Different types of employees—volunteers, state and local outreach staff, campaign leadership, candidates—require access to different resources. Having predetermined profiles makes it easier to ensure that people are getting access only to what they need.

WHAT ARE ADMINISTRATORS?

In "IT speak," an "administrator" or "admin" has the ability to give people access or control to systems or information. For example, as the "admin" for an email system, you can create accounts, change passwords, and set requirements like password length and two-factor authentication for all accounts. In an office suite like GSuite or Microsoft 365, you can also create groups, such as the "GOTV Team" or "Comms Team." An admin's job is really important. If they do things right, information will be available only to people who need it, which is essential for security. This means that deciding who gets admin privileges is also a critical decision. Only a few, highly trusted and trained people should be able to grant others access to information. If a staffer with "admin" privileges leaves the party or campaign, make sure to take away their privileges immediately!

Step 4: Incident Response Planning

It's just as important to plan for responding to an attack as it is to develop a security strategy to prevent one. How you respond often has more to do with the ultimate outcome of an incident than what was compromised. You should budget some time with senior leaders or management to discuss what will happen if something does go wrong. Here's a checklist of the steps you should take:

LEGAL

Identify outside counsel you will retain in the event of a cyber incident, and discuss the response process with them at the outset of the campaign. In most cases, this will be the same person who represents your campaign on other matters, but ideally you would have someone who specializes in incident response on call, either pro bono or for a $0 retainer. This becomes increasingly important as India adopts more legislation related to cybersecurity and data privacy of its citizens.

Ask your lawyer to explain your legal obligations if data is stolen and what compliance measures you will need to have in place.

Understand your vendors' legal obligations to notify you or others if they are hacked. Wherever possible, include strict notification requirements in your vendor contracts, since third parties are a frequent source of breaches.

If you believe you've been breached, a best practice is for your lawyer to oversee your response under attorney-client privilege.

Talk to your lawyer about the best way to work with law enforcement if a breach occurs. Every campaign will approach this differently.

TECHNICAL

Determine ahead of time whom you will call for technical assistance if you think you've been hacked. Ideally, get a placeholder contract set in advance.

Choose someone on the campaign who will interface with technical experts in the event of a breach. This is ideally the same person who is already coordinating IT. Managing an incident response can be overwhelming, so you want someone focused on the technical aspects who knows what they are doing. That way you can focus on communicating with stakeholders and the press.

Learn about the technical assistance or other support that the platform providers can give you in the event of a cyber incident such as a hack or other attack.

OPERATIONS

Decide in advance who will be on your Incident Response Team (IRT) and who will participate in incident response meetings. It's important to include someone from your IT, legal, operations, and communications teams. If you don't have full-time communications, IT, or operations support, plan to include any key staff who oversee campaign operations.

Determine the chain of command for decision-making in the event of a breach, especially regarding communications. In many cases, this will be the campaign lead, but some leadership may choose to delegate responsibility to someone else. Write down that decision-making tree and make sure those who are part of it understand their roles.

Identify what app or technology you will use to communicate if you think your systems have been breached. For example, if your email is hacked, you may want to rely on a secure messaging app such as Signal or WhatsApp. Communication during a breach is essential, but you don't want your adversaries to know what you're saying—or even that you are responding to their actions.

COMMUNICATIONS

Identify key internal and external stakeholders, like your staff, volunteers, donors, and supporters. Know whom you need to contact if an incident occurs and rank them in order of priority. Develop a contact list, methods for quick and easy contact and designate who will reach out to them.

Conduct scenario planning. Brainstorm the most damaging scenarios and consider how your stakeholders and messaging may change for each one. Pick roughly five to plan against. Different scenarios could include:

- Your social media accounts are taken down, hacked or faked;
- A misinformation campaign is launched against your party, campaign or candidate, including deep fake videos and stolen emails;
- A rogue staffer or volunteer leaks sensitive information to the press;
- Rumors surface that your party or campaign has been hacked;
- Personally identifiable information of supporters and donors is leaked;
- Ransomware and an extortion attempt are lodged against your party and campaign;

- Your adversary steals your administrator's credentials and every sensitive party strategy document;
- Your party or campaign website is taken down;
- The internet is cut, or particular sites, apps or protocols are blocked nationwide.

Be careful what you say now about cybersecurity policy or cyber incidents. Some victims of cyber crimes have previously made grandiose pronouncements about their own security measures, or have criticized others who have been attacked. The press will hold you accountable for what you said in the past if you fall victim.

Similarly, avoid providing details about the scope of the event, especially in the early phases of the incident, and if you can avoid discussing the scope altogether, even better. Details available at the outset will change as you investigate. A common mistake is to say something that later turns out not to be true (e.g., "they didn't steal very much," or "no personal information was taken"). Saying only what you know for sure is the safest course. Statements should focus on the actions you are taking to make the situation right for the affected stakeholders.

Develop some boilerplate language in advance, ideally in consultation with your legal representatives, so that you can draft statements or talking points quickly if an incident occurs. If possible, tailor it in each of the five scenarios you choose to plan against. At a minimum, create a simple Q & A document that you can rapidly revise if you actually need to use it. Creating a Q & A document in advance will help you to think as much about what you won't say as what you will say. For example, the first question will often be, "What happened?" However, you may not be able to answer that for days or weeks. The fact that you don't know what kind of breach will take place can actually help you write better boilerplate answers in advance.

Be sure that your talking points are communicated as clearly and quickly as possible to state and local-level representatives. This communication should be constant from the outset of your campaign, not just when crisis occurs. It is important that the party and campaign be on the same page at all levels.

QUESTIONS TO INCLUDE IN YOUR Q&A DOCUMENT:

- What happened?
- How did it happen?
- Who did it?
- What was stolen or damaged?
- Was anyone's personal information stolen? What are you doing to protect them?
- How did the hackers do it?
- Are the hackers out of your system?
- How long were they in your system?
- What security measures did you have in place? Why weren't they effective?
- Shouldn't you have known this would happen? Why weren't your systems better secured?
- Are you working with law enforcement? Has law enforcement contacted you?
- In a ransomware breach, you'll be asked: Did you pay the ransom and why or why not?

Stay in touch with your key stakeholders and keep them as informed as you can. You probably won't be able to say much, but contacting them regularly with what you do know, having a clear statement about your intentions, and providing details about what you are doing to manage the situation are key. Avoid setting an expectation of too frequent updates, because often you won't have new information and your stakeholders will become frustrated if you continue to return to them without new information. Only speak proactively to the media if you have new information to provide.

For additional, detailed guidance on incident response communications planning, check out the International version of the **Election Cyber Incident Communications Plan Template**.

Step 5: Devices

Every physical device in your party and campaign—from a cell phone, tablet, or laptop to a router, printer, or camera—represents a potential attack path into your network. A good cybersecurity plan will attempt to control access to, into, and on all devices. You can control access to devices by making sure they are always properly handled and accounted for. You control access into devices via two-factor authentication and strong passwords. You control the content on devices via encryption and the policies guiding how you store data (i.e., storing information in the cloud instead of on machines).

GOOD — What You Need to Do

1. Always use the most updated operating system (OS) available, since system updates regularly include patches for the latest vulnerabilities. If possible, set device settings to auto-install these updates. Make it someone's job to check on a regular basis that everyone is current.

2. Have a backup! For any data that you keep stored on a local device (your PC, for example), be sure to have a backup plan in case of physical theft, in case your computer breaks, or you spill coffee all over the keyboard. For example, you can use an automatic cloud-based backup service to mitigate the impact of data loss. Examples include Backblaze and CrashPlan.

3. Access to the device

    a. From the start, leadership should create an environment in which people take physical security of their devices seriously—losing a device could give an adversary access to critical information that can be used to hurt the party and campaign.

    b. Although many campaigns cannot afford to buy new devices, it's always best to purchase new equipment (especially computers and phones) if you can. At a minimum, you should provide new devices for personnel who work with sensitive data or at a minimum erase and reinstall the operating system on those old devices. If staff and volunteers are using their own computers and phones, establish a "Bring Your Own Device" (BYOD) policy that implements strong security practices (see endpoint protection below).

    c. Campaign staff and volunteers should NOT use personal email accounts or devices that have not been secured per the BYOD policy for campaign business, including email and social media. Any important information that resides outside devices or systems controlled by the campaign is vulnerable to attack. Leadership should constantly reinforce that party and campaign data needs to stay off personal email and unsecured computers.

d. Maintain the physical security of your devices. When on public transportation, at a cafe, or even in your office, always take steps to prevent the theft of devices that could give access to your accounts, communications, and data.

e. Report lost devices immediately. Require default settings that allow for remote wiping on all devices. Example include Find my iPhone, and Android Device Manager.

f. Win or lose, have a plan in place for what happens to all data, accounts, and devices when a campaign ends. The immediate aftermath of a campaign is an especially vulnerable period.

4. Access into devices

a. Change default passwords and settings on all devices. Many devices come from the factory with a default password that is really easy to guess. Also, disable the guest account if a device comes with one.

b. Implement auto-lock for phones and computers after at most two minutes and require a password or fingerprint ID to unlock.

c. Turn on auto-wipe for your mobile devices so that they will erase themselves after a certain number of failed login attempts.

5. Content on devices

a. Require encryption on all devices (computers and phones) to ensure that the loss of a device does not mean the compromise of its content. Examples include FileVault for Mac and BitLocker for Windows. Some devices like the iPhone do this by default, but not all do.

b. Install endpoint protection software on all devices. Some examples include Trend Micro, Sophos, and Windows Defender. There are special endpoint security apps for phones and tablets, such as Lookout.

WHAT IS ENDPOINT PROTECTION?

Endpoints are the devices that staff use, including mobile phones, laptop computers, and desktop computers. They are the "endpoints" of the campaign's network, and staff are the "end users." Endpoint protection centrally controls and manages security on remote devices. It's especially important for campaigns that allow staff to "bring your own device" (BYOD), since the campaign needs to ensure that the device is secure, free of malware, and can be wiped if stolen or lost. Endpoint protection can also monitor the device to make sure software is up to date and detect new malware or potential threats. For many parties and campaigns, this will feel like a big lift, but building it into your routine onboarding and investing some time upfront can save you a lot of grief later.

ENHANCED — Take the Next Step

6. Use mobile device management (MDM) software, which monitors activity to ensure all devices comply with the mobile phone and user device security policies you have established for your party and campaign. Examples include VMware AirWatch, Microsoft InTune, and JAMF. GSuite and Microsoft Office 365 also include an MDM service.

7. Use advanced threat protection services that monitor and alert for malicious activity, such as CrowdStrike Falcon or Mandiant FireEye. Crowdstrike sometimes offers Falcon breach prevention service pro bono through the Crowdstrike Foundation, depending on the needs of your campaign and campaign finance rules.

Step 6: Networks

Networks are the system of physical hardware, digital software, and their connections. They represent another target-rich environment for attack. Network security comprises everything from how devices communicate with one another to using cloud services for data storage.

GOOD — What You Need to Do

1. Store data on trusted cloud services, not on personal computers or servers. Anything stored on a personal device faces higher risk from hackers, theft or accidents than data stored in the cloud.
    a. No one should have access to all files on the network; accounts with comprehensive administrator access should not be used for day-to-day work. Divide your file storage into department folders and grant access accordingly.
    b. Ensure access to shared content is by invitation only. Some file management services also allow for implementing expiration dates on invitations and access.
    c. Periodically audit what is being shared and with whom.
2. Have a separate "guest" wifi network for visitors and volunteers that limits their access to party and campaign resources. Try to purchase routers that offer a "guest profile" that will automatically segment your network. We strongly suggest changing the network password at the end of campaign events when there might be a large turnover of staff and volunteers.
3. Avoid public wifi services as much as possible and use trusted wifi networks wherever possible. If you need mobile wifi, then try to provide party and campaign staffers with mobile wifi hotspots for tethering. Public wifi is often free and easy to connect with, but attackers can also use it to penetrate your hardware.
    a. Where possible, staffers should use a VPN (virtual private network). VPNs help protect against intruders when on public wifi. Examples of VPN services include ExpressVPN or TunnelBear. Not all VPNs are created equal. Beware of free services: many are looking to take your data!
4. Secure your browser. PC Magazine ranked Chrome and Firefox as the two safest browsers in 2017. Regardless of what browser you use, keep it up to date.

WHAT ARE VPNS?

A virtual private network (VPN) is an encrypted "tunnel" for your internet traffic, hiding it from intruders. Some offices use it as a way to log remotely into the office network, but this isn't very common for campaigns. Parties and campaigns should consider having their staff use a VPN on computers and mobile phones if they often have to use public wifi or untrustworthy networks (which is sometimes the case for traveling staff or state and local offices). Google has recently released a new do-it-yourself VPN system called Outline.

ENHANCED — Take the Next Step

1. You can take more advanced steps to protect your network, but they should be implemented by an IT professional. We would suggest you ask them to include the following:
    a. Set up a hardware firewall.
    b. Encrypt your wifi connection using the WPA2 or 802.1x security protocols (do not use WEP).
    c. Configure cloud-based web proxies to block access to suspicious sites from any party-owned device, no matter where it is. Service provider examples include Zscaler, Cisco Umbrella and McAfee Web Gateway Cloud Service.
    d. Have your activity logs stored on a cloud service provider such as LogEntries or SumoLogic.
    e. Segment your cloud-based storage so that not everything is stored in the same place. Opposition research, strategy memos, and personnel files should be kept in different folders, and access to those folders should be restricted to the people who really need them. Consider a different storage system entirely for your party and campaign's most sensitive information. Restrict access so that only key personnel can access it, and only when using specific devices. (For example, if you use Microsoft365 for your office suite and document storage, put your most sensitive documents on a Dropbox or Box account.) If a party or campaign staff member becomes compromised, this kind of segmentation can limit the damage.
2. Train staff and volunteers not to connect their devices to unknown ports or devices. Don't use public chargers at airports or events. Don't accept free phone chargers or batteries at events (that free USB drive may be loaded with malware!).

Step 7: Information Operations and Public Facing Communication

Information operations have been in the news a lot recently, especially those campaigns run by foreign intelligence services and domestic political opponents. It will be up to elected leaders and policymakers to decide how to confront information operations moving forward, but there are a few things we can do to manage them if they're happening. Parties and campaigns have and will continue to be targets of these operations and need to be prepared. Defending how your campaign communicates with the public is an important part of this. Below are some ways to better protect against information operations, identify when they are happening to your campaign or candidate, and respond quickly when they do occur.

WHAT ARE INFORMATION OPERATIONS?

Information is power--or at least that's what a lot of military and intelligence services think! The power of ideas has long fueled rebellions, insurgencies and civil wars and many countries that may have inferior military capabilities in the traditional sense seek to use information to divide and pre-occupy their adversaries. In Russia, for example, influencing public opinion through propaganda and inflaming local tensions is part of their doctrine of warfare and something they practice constantly on perceived adversaries. Social media completely changed the information operations game. It's now easier than ever to move information quickly and impersonate other people, creating the impression of public anger or division. Targeted information operations occur in the domestic political space as well.

GOOD — What You Need to Do

1. Remember: information operations are a communications problem, not a technical one. Adversaries can make their information operations more potent by stealing your data, but once information is out in the environment - whether that be TV, print, WhatsApp, Facebook, Twitter, etc. -you need a communications strategy to manage it. Think in advance how to handle fake or slanted news--will you ignore it or counter it with true and accurate information? Re-post it and reinforce that it's false? How will you make this decision? These are among the most difficult decisions any party and campaign has to make, but

what matters most is think about these questions with your team in advance, so you and your team have guidance about how to respond, if you respond at all. It is also important to ensure that these guidelines and protocols are distributed to party and campaign staff and volunteers at the state and local level, since communications aren't centralized at headquarters.

2. Establish yourself as a credible source of accurate information on the election and campaign process. If the party and campaign are seen as credible courses of information, you will be in a much better position to counter false or misleading information.

3. Know what's going on. Encourage activists to share posts, sites, or news stories they find suspicious. If you want, you can deputize some volunteers to focus on this specifically, conducting searches to find out what content is out there. One ongoing challenge is that it's impossible to see everything that voters may be getting on their Facebook feed or WhatsApp channels. The best way to solve this right now is to deputize a team of volunteers, who represent different geographies, languages and demographic groups in your party and campaign, so you can catch as much as possible.

4. Establish contact with key social media platforms and notify them if you find fake or misleading information. Most social media platforms will now remove "fake" or misleading content and imposter profiles. Ensure that party and campaign leadership establish a point of contact at social media platforms and establish contact early in the campaign so you can reach out quickly if something goes wrong. Be sure that leadership at the state and local level also have these contacts - or create a mechanism for all branches of the party and campaign to report platform-related issues to a central point-person.

5. Monitor for imposter sites or apps. To-date, there are no public reports of imposters trying to steal money or activist data through fake websites or party/candidate mobile apps, but it's such an easy vector of attack, you should be on the lookout. Make sure to purchase any web addresses you may want to use (or could be used against you). If you want, you can retain a reputation management service that will monitor the web for you. Some can do this at a fairly modest price.

6. Protect Against a Distributed Denial of Service Attack (known as DDoS). A DDoS attack is when an adversary takes control of a lot of machines, and uses them to "ping" your website all at once, causing it to crash. Most of what we focus on in this guide is how to keep people away from your party and campaign data, but, in the case of a DDoS, you want to keep your website open and available all the time for donors, voters and activists. DDoS could be used to block you from fundraising or simply cause a really frustrating disruption to your campaign. There are two free tools you can use to protect your site, Google Shield and Cloudflare.

Do you see a way to make this Playbook better?

Are there new technologies or vulnerabilities we should address?

We want your feedback.

Please share your ideas, stories, and comments on Twitter @d3p using the hashtag #CyberPlaybook or email us at connect@d3p.org so we can continue to improve this resource as the digital environment changes.

Defending Digital Democracy Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/D3P