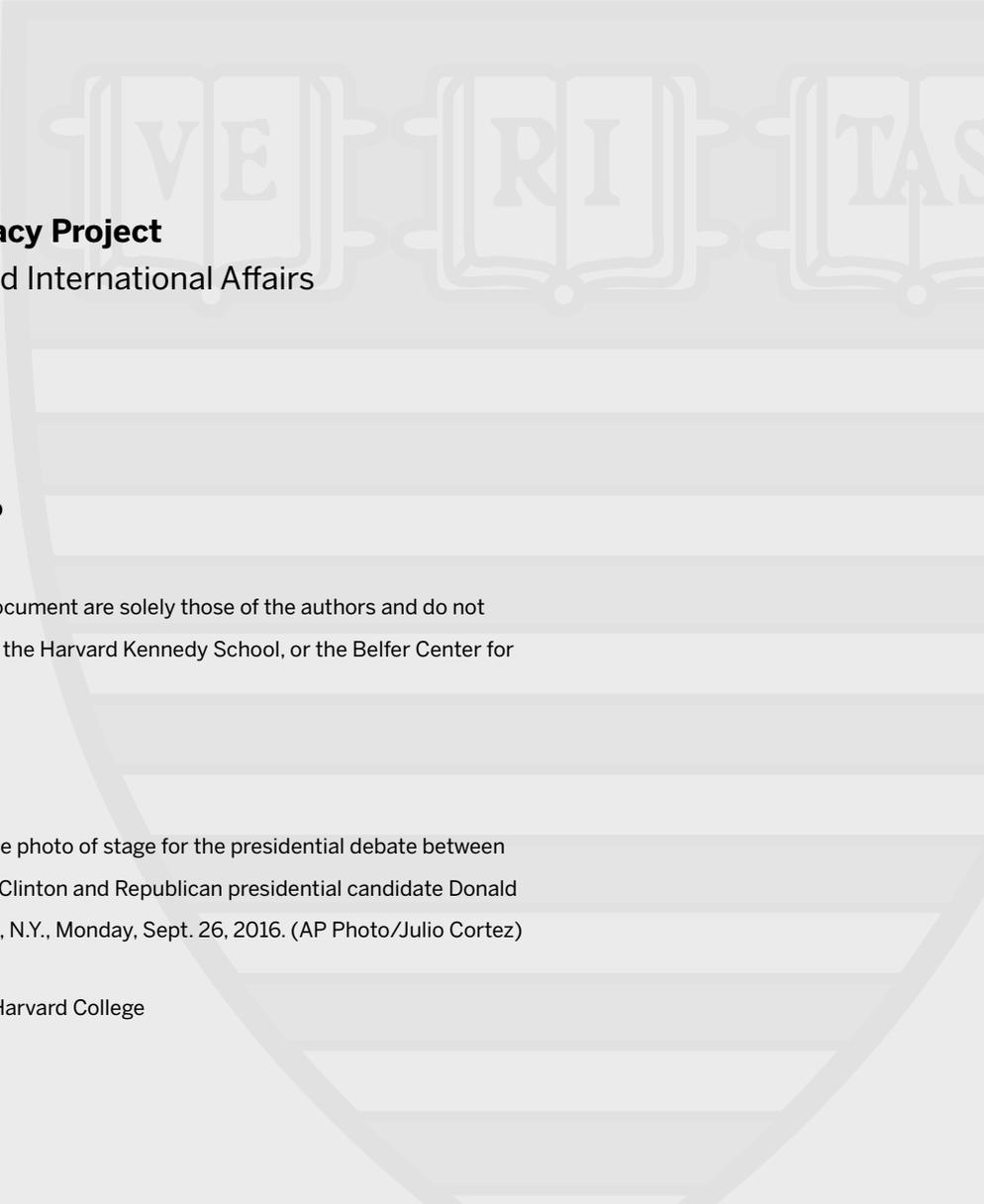


The Cybersecurity Campaign Playbook



HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

DEFENDING DIGITAL DEMOCRACY
MAY 2018



Defending Digital Democracy Project

Belfer Center for Science and International Affairs

Harvard Kennedy School

79 JFK Street

Cambridge, MA 02138

www.belfercenter.org/D3P

Statements and views expressed in this document are solely those of the authors and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design & Layout by Andrew Facini

Cover photo: Lena Gjokaj takes a cell phone photo of stage for the presidential debate between Democratic presidential candidate Hillary Clinton and Republican presidential candidate Donald Trump at Hofstra University in Hempstead, N.Y., Monday, Sept. 26, 2016. (AP Photo/Julio Cortez)

Copyright 2018, President and Fellows of Harvard College



The Cybersecurity Campaign Playbook

Contents

- Welcome 3**
 - Authors and Contributors 4
 - The Playbook Approach 5
- Introduction 5**
 - The Vulnerable Campaign Environment 7
 - The Threats Campaigns Face 8
- Managing Cyber Risk 9**
- Securing Your Campaign 10**
- Top-Five Checklist 12**
- Steps to Securing Your Campaign 13**
 - Step 1: The Human Element 13
 - Step 2: Internal Communication 17
 - Step 3: Account Access and Management 19
 - Step 4: Devices 22
 - Step 5: Networks 25
 - Step 6: Information Operations and Public Facing Communication 27
 - Step 7: Incident Response Planning 29

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.

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 American 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 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.

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 our 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

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.

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

Dai Lin, D3P, Harvard Kennedy School

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

BELFER CENTER WEB & DESIGN TEAM

Arielle Dworkin, Digital Communications Manager, Belfer Center

Andrew Facini, Publications and Design Coordinator, Belfer Center

The Playbook Approach

A bipartisan team of experts in cybersecurity, politics and law wrote this *Cybersecurity Campaign Playbook* to provide simple, actionable ways of countering the growing cyber threat.

Cyber adversaries don't discriminate. Campaigns at all levels—not just presidential campaigns—have been hacked. You should assume that you are a target. While the recommendations in this playbook apply universally, it is primarily intended for campaigns that do not have the resources to hire full-time, professional cybersecurity staff. We offer basic building blocks to a cybersecurity risk mitigation strategy that people without technical training can implement (although we include some suggestions that 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 campaigns to enlist professional input from credentialed IT and cybersecurity professionals whenever possible.

Introduction

Candidates and campaigns face a daunting array of challenges. There are events to organize, volunteers to recruit, funds to raise, and the relentless demands of the modern media cycle. Every staffer must anticipate unfortunate surprises like gaffes or a last-minute attack ad. Cyber attacks now belong on this list as well.

As campaigns have become increasingly digital, adversaries have found new opportunities to meddle, disrupt, and steal. In 2008, Chinese hackers infiltrated the Obama and McCain campaigns, and stole large quantities of information from both. In 2012, the Obama and Romney campaigns each faced hacking attempts against their networks and websites. In 2016, cyber operatives believed to be sponsored by Russia stole and leaked tens of thousands of emails and documents from Democratic campaign staff.

The consequences of a cyber breach can be substantial. News of a breach itself, compounded by a slow-drip release of stolen information, can derail a candidate’s message for months. Attackers overloading a website can lead to lost donations at key moments. The theft of personal donor data can generate significant legal liabilities 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 president or city council.

For the foreseeable future, cyber threats will remain a real part of our campaign process. As democracy’s front line, 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. Ironically, 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 *Cybersecurity Campaign Playbook*.

In today’s campaigns, cybersecurity is *everyone’s* responsibility. Human error has consistently been the root cause of publicized 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 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 are often onboarded quickly without much time for training. They may bring their own hardware from home and the malware lurking on it. Events move quickly, the stakes are high, and people feel that they don't have time to care about cybersecurity. There are a lot of opportunities for something to go wrong.

At the same time, campaigns rely more and more on proprietary information about voters, donors, and public opinion. They also store sensitive documents like opposition research, vulnerability studies, personnel vetting documents, first-draft policy papers, and emails on various servers. 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, fire up the coffee maker, 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 cool million in Bitcoin and 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' Social Security numbers. The group has spent weeks combing through the bounty in search of dirty laundry and created an easy-to-use website dedicated solely to distributing the highlights. Prominently featured is a lengthy "self research" book on your candidate. For now, the campaign's website is down, its social media accounts 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 our country, foreign adversaries may think that harming or helping a particular candidate advances their national interest, whether that means creating chaos and confusion among American voters, or punishing an official who has spoken out against them. This may sound like thriller fiction, but the reality is that a sophisticated foreign 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 managers and staffers have to realize are possible.

WHO'S HACKING?

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. The Chinese have focused much more on information gathering. They are believed to have been active in the 2008 and 2012 presidential campaigns, but there is no evidence they released any stolen materials. The North Koreans famously retaliated against Sony Pictures Entertainment for producing the film, *The Interview*, by stealing and releasing company emails and wiping their systems. Heightening tensions with the United States could prompt more attacks in the future.

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. Then there are actual **threats**: the nation-states, 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 little you or your campaign can do to prevent threats themselves—they are the result of larger geopolitical, economic, and social forces. What you *can* do is substantially reduce the likelihood that your adversaries will succeed by reducing your own vulnerability. Reducing vulnerability reduces risk—it's up to you to decide which ones are most essential to address based on the possible consequences. For example, you may decide that the most damaging thing a hacker could do is to steal your candidate's self research report. In response, you devote extra resources for secure cloud-based storage, use two-factor authentication, and restrict access to a small number of people. You may decide to make other documents on the campaign more widely available and less secure, since more people need them to do their jobs and they wouldn't cause much damage if they were leaked.

There are technical aspects to risk mitigation, but what matters most is that you take a holistic approach. As a campaign leader, you must make fundamental choices, such as who has access to information, what information is kept or discarded, how much time you devote to security training, and how you behave as a role model. As a campaign professional, 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 them.

Securing Your Campaign

Our security recommendations are organized according to three principles:



Prepare

The success of nearly every one of the *Playbook's* recommendations depends on the campaign manager creating a culture of security vigilance that minimizes weak links. That means establishing clear ground rules that are enforced from the top down and are embraced from the bottom up.



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 data security works best in layers: there is no single, bulletproof technology 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.



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. 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 campaign *must* do to have a *minimum* level of security. Using the “good” recommendations in a piecemeal fashion will leave you vulnerable. 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.

Management

Campaign managers need to take responsibility for their cybersecurity strategy, but most will delegate development and supervision to a deputy or operations director. It's important that cybersecurity is tightly integrated into HR and IT work, since correctly onboarding staff, provisioning hardware, and controlling permissions will be critical to your strategy. Many small campaigns will rely on volunteer support for IT and cybersecurity. You can use this playbook to guide your discussion with your volunteer support. The key is to carefully vet the volunteers who support you and carefully control access, so that volunteer support doesn't create new vulnerabilities. You should make sure a campaign staffer is supervising IT work and controlling permission to access different systems.

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, even if there are just one or two staff, then complete the other “good” recommendations as soon as possible.

Cost

A lot of what we recommend here is free or very low cost. In fact, everything on our top five list is free, except getting a cloud-based platform, which will only cost a few dollars per month per employee. 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 multi-million dollar statewide 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. You are responsible for reducing risk, training your staff, and setting the example. Routinely update and patch all systems. Human error is the number one cause of breaches. Phishing continues to be a leading method of attack. Train your staff to be on guard for suspicious messages. *(see page 12)*

2. Use the cloud:



A big, commercial cloud service will be much more secure than anything you can set up. Use a cloud-based office suite that will provide all your basic office functions and a safe place to store information. *(see pages 14-15)*

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



Require 2FA 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 text messaging. *(see pages 16-17)*

For your passwords, using a password manager is the best way to reduce risk. They allow you to generate and store long and random passwords that you don't have to memorize—the program does that for you. If for some reason you don't use a password manager then 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\$. *(see page 17)*

4. Use encrypted messaging for sensitive conversations and materials:



Using an encrypted messaging tool for phones like Signal or Wickr 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 as possible. *(see pages 19-22)*

Steps to Securing Your Campaign



Step 1: The Human Element

Cybersecurity is fundamentally a human problem, not a technical one. The best technological 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 on creating a culture of security awareness.

“Good” — What You Need to Do

- 1. Establish a strong information security culture** that emphasizes security as a standard for a winning campaign. Just as campaign staffers are instructed not to take an illegal donation, employees 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. You can distribute the *Staff Handout* at your training.
 - b. Trainings:** Make security part of all your ongoing **staff trainings**, such as senior staff retreats or GOTV trainings. Provide **additional training** for those in sensitive roles, such as the candidate, press staff, senior staff, and anyone with system administrator privileges on your network. Managers should require that the most important people in the campaign—including the candidate—have their security settings checked by whoever runs IT (that may be the manager herself).
 - c. Set the example:** Senior campaign staff and the candidate must take a **visible leadership role**, advocating for cybersecurity during trainings. Senior staff should provide **periodic reinforcement** of cybersecurity's importance to junior staff in meetings and on calls. Don't just have technical experts conduct trainings. The campaign manager or operations director can be a more powerful messenger precisely because they're seen as less “technical.”
- 2. Train and educate your staff to be on the lookout for phishing.** Phishing attacks against campaigns are on the rise and continue to be a primary method used by malicious actors. Train your staff to be suspicious of any email asking for information, or claiming they need to click a link to reset their credentials. Sophisticated phishing attacks may come from spoofed or compromised senders that appear legitimate. Encourage staffers to share anything suspicious with you or your IT staff. The more people share, the more confident you can be that they're being vigilant and the more

intelligence you will have. The overall rule of thumb should be to “think before you click”, but we’ve included three key points you can remind you staff about when you train and re-train. Training should emphasize best practices such as ‘hovering’ over a link to identify the actual url, expanding email details to confirm the email address of the sender, and using a different communications channel such as a quick phone call to confirm authenticity of the sender and email contents 2FA is another important way to prevent a spear-phishing attack from leading to an account compromise—just having your username and password will not be enough to access your account. As part of the campaign’s strong security culture, senior staff should recognize and praise anyone who reports suspicious behavior on their system or admits to clicking a potentially malicious link.

- a. **Phishing can happen on the phone, too!** Staff should never share information, wire money, or give anything else away on the phone if they aren’t certain who the caller is. Make staff aware of the threat and tell train them to listen to how the caller greets them and to ask questions that outsiders may not be able to answer. You can easily test your staff on phishing calls—and your friends will enjoy doing it!

3. **Conduct a thorough vetting** of staff, volunteers, and interns—anyone requesting access to campaign information—to avoid giving credentials to someone who wants to steal or sabotage your systems. 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.” 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).
4. **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).
5. **Control access** to important online services, such as the official campaign social media accounts, to prevent use by unauthorized individuals. Make sure that those who leave the 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.

“THINK BEFORE YOU CLICK”

PAUSE before you click on a link within an email to check what address the email is coming from and to ask yourself if the email is suspicious.

CONFIRM that a request for information, money, personal information, passwords, documents, etc. is legitimate by following up with the person requesting, ideally in person, or at least by phone. Never give your password or personal information over a link.

REPORT anything suspicious to your leadership by forwarding any email that's remotely questionable. Make sure you flag it as “suspicious” (e.g., in the title) so that no one else inadvertently acts on a malicious email.

From: MS Enterprise E-mail <bm@pro-f.dk>
Date: Wednesday, March 14, 2018 at 12:19 PM
To: [Redacted]
Subject: Email Notification : [Redacted]

Not a Microsoft Domain



Hello [Redacted] — Salutation to email address, not full name

You have some malicious files in a hidden folder and such files are against our Term of service (T.O.S)

In order for us not to terminate your email service these files must be deleted automatically.

Kindly remove all hidden files automatically below.

Link to “take action” does not go to Microsoft or Office365 — [REMOVE HIDDEN FILES](#)

Thanks for taking these additional steps to safe guard your email.

© 2018 Outlook Corporation. All rights reserved. | Acceptable Use Policy |

“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 counseling and 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 campaign’s systems and an IT security expert to help protect, maintain, and monitor your campaign’s 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, U.S.-based firm—not all cybersecurity firms provide the same level of service.

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: Internal Communication

Not all methods of communication are equally secure, so use the most secure method possible. Campaign leadership should set a standard that encourages in-person conversations whenever possible, and discourages needless or superfluous emails. 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 a cloud-based office suite** that provides secure email communication, document creation, chat, and file sharing, such as GSuite or Microsoft365. For GSuite Enterprise, choose “Advanced Protection” and for Office365, use E5. Both will have built in settings that are more secure. 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. Cloud-based systems managed by major firms will be better protected than any servers you could set up in your campaign. There are free versions of both products, but the paid versions give you many more administrative capabilities. Google’s Advanced Protection Program provides extra security against targeted online attacks like phishing (this is available for their consumer Google/Gmail accounts). Through Google’s Protect Your Election effort, they also offer a free service to protect your website against disabling attacks.

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 in the cloud instead of on your personal computer because reputable cloud service providers have the money and expertise to make their server farms more secure than your laptop’s hard drive, or an office server. It’s like the difference between leaving cash under your mattress and storing it in a bank’s security vault. Using reputable 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.

2. **Use the most secure systems possible for communication.**
 - a. Use encrypted messaging services such as Signal, Wickr, especially for messages, document sharing and phone calls. Many campaigns require that sensitive information *only* be transmitted by encrypted messaging, although you can use it for all communication if you want (this is especially smart for high-risk individuals like the candidate). Signal and Wickr allow you to auto-delete messages, which reduces risk.
 - b. Switch off archiving for messaging services, such as Google Chat and Slack, 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.
3. Defend 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.
4. Secure personal accounts
 - a. Campaign business should never go on personal accounts. However, adversaries will target personal accounts for hacking, so have your staff use strong passwords and two-factor for their personal accounts as well (this is included in our *Staff Handout*).

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 or Wickr, make the process seamless. Laptops or cloud storage systems use encryption as well.



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 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.

“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 well as texting, 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. As malicious actors evolve their methods, we are seeing advanced attack techniques used to phish second factor codes sent to users. We strongly encourage the use of physical security keys for two-factor authentication, as they are not vulnerable to phishing. The website “TwoFactorAuth.org” is a helpful guide to services that do and do not offer 2FA.

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.

2. Passwords

- a. **Ensure no systems are using default usernames or passwords**—this is a commonly overlooked error. Make sure each system and user has their own unique username and password,
- b. **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.

- c. **Use a different password for different accounts** so a hacker can't break into multiple accounts if a single password is stolen.
 - d. **If someone reaches out requesting a password or password reset, require the request to be made in person or over a video chat** to ensure it is the actual campaign staff member or volunteer. Only share passwords in person or over short-lived encrypted messages. Never share passwords over email or store/distribute using a helpdesk system.
3. **Use password managers** 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, which are often less secure than these standalone managers.

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. For campaigns, password managers sometimes make sense for accounts that have multiple users, because the administrator can safely share access to them.

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 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 campaign. Immediately change passwords if suspicious activity is observed.

6. **Use encrypted messaging for sensitive information.** The federal government has confirmed the presence of “stingray” machines that can intercept cellular data, especially in the Washington, DC area. This is yet another reason to keep communications on encrypted messaging apps, which will be unreadable even if your signal is intercepted.
7. **Monitor all campaign, staff, and related social media accounts.** It is important to identify and respond quickly if you have been hacked. In line with the “Prepare, Protect, Persist” framework, campaign leadership should create a response plan for this scenario. This response plan should include finding appropriate points of contact within each social media company to get in touch with in the event that campaign accounts are hacked.

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 “Field 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 people should be able to grant others access to information. If a staffer with “admin” privileges leaves the campaign, make sure to take away their privileges immediately!

“Enhanced” — Take the Next Step

1. **Create user profiles for different types of campaign staff that automatically grant the necessary level of access.** Different types of employees—interns, field staff, campaign leadership—require access to different resources. Having predetermined profiles makes it easier to ensure that people are getting access only to what they need.



Step 4: Devices

Every physical device in your 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. **Use an automatic cloud-based backup service** to mitigate the impact of data loss if a device is lost or stolen. Examples include Backblaze and CrashPlan.
3. **Physical access to the device**
 - a. From the start, campaign 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 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.
 - c. If staff are using their own computers and phones, **establish a “Bring Your Own Device” (BYOD) policy** that implements strong security practices (see endpoint protection below).
 - d. Campaign members 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 campaign data needs to stay off personal email and unsecured computers.
 - e. Report lost devices immediately. Require default settings that allow for **remote wiping** on all devices.

- f. Win or lose, have a plan in place for what **happens to all data, accounts**, and devices when the campaign ends. This includes thinking how to safeguard or erase data at the hardware level. Reformatting a hard drive is not enough to protect your data. Residual data on reformatted or disposed drives can be obtained using commercially available forensics software. Extremely sensitive data should be degaussed or melted. The immediate aftermath of a campaign is an especially vulnerable period.

4. Digital 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 two minutes and require a **password** or fingerprint ID to unlock.

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. Require all consultants to keep data on their machines encrypted as well.
- 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. Lookout is an example.
- c. Limit what apps can access on all devices. This means limiting what apps are installed and limiting permissions for those apps (e.g., limiting access to contact lists or location and GPS information, turning off 'always active' mode).

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 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

1. **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 campaign. Examples include VMware AirWatch, Microsoft Intune, and JAMF. GSuite and Microsoft Office 365 also include an MDM service.
2. **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 5: 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. Embrace the cloud.** Store data on cloud services, not on personal computers or servers. Anything stored on a personal device faces higher risk than 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 campaign resources. Try to purchase routers that offer a “guest profile” that will automatically segment your network.
- 3. When traveling, or before you set up your campaign office, avoid public wifi services as much as possible** and use trusted wifi networks wherever possible. If you need mobile wifi, then try to provide 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.

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. 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 field offices).

“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 campaign-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 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, but your most sensitive documents on a Dropbox or Box account.) If a member of the campaign becomes compromised, this kind of segmentation can limit the damage.
2. **Train staff 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 6: Information Operations and Public Facing Communication

Information operations have been in the news a lot recently, especially campaigns run by foreign intelligence services to influence opinion in the United States. It will be up to elected leaders and policymakers to decide how to confront information operations moving forward and there's little we can do as campaign staff to impact whether they happen or not, but there are a few things we can do to manage them if they're happening. Campaigns have and will continue to be targets of these operations and need to be prepared. Defending ways 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 how to 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 every to move information quickly and impersonate other people, creating the impression of public anger or division.

“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, you need a communications strategy to manage it. Think in advance how to handle fake or slanted news—will you ignore it? Re-tweet it and reinforce that it's false? How will you make this decision? These are among the most difficult decisions any 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.

- 2. Know what's going on.** Encourage activists to share posts, sites, or news stories they find suspicious. If you want, you can deputize some interns or 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 feeds. The platform has made it harder to post political advertising and has increased staff to monitor news content, but you cannot search all content. The best way to solve this right now is to deputize a team of volunteers, who represent different geographies and demographic groups in your state/district, so you can catch as much as possible.
- 3. 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. Ask your relevant campaign committee or state party for the best contact at social media platforms and establish contact early in the campaign so you can reach out quickly if something goes wrong.
 - a. Facebook
 - b. Twitter
 - c. Google/YouTube
- 4. Monitor for imposter sites.** To-date, there are no public reports of imposters trying to steal money or activist data through fake websites, 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 [do we include examples?]. Some can do this at a fairly modest price.
- 5. 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 campaign data, but, in the case of a DDoS, you *want* to keep your website open and available all the time for donors and activists. DDoS has not yet become a common threat to campaigns, but it 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's Project Shield and Cloudflare.



Step 7: 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 at strategic retreats or longer senior staff meetings 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.

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. Your state caucus or national party committee can usually provide referrals.

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 for the campaign. 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.

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're a small campaign and 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 manager, but some managers may choose to delegate responsibility to someone else.

Identify **what app or technology you will use to communicate** if you think your email has been breached (Signal and Wickr are two common options). 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:

Conduct scenario planning. For many campaigns, this can be part of an existing strategy retreat. For bigger campaigns at higher risk, it may be necessary to have a dedicated meeting. Your scenario planning should include:

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 and designate who will reach out to them.

Understand of the different types and varying sensitivity of the data you're collecting. Think through what could happen if the data is no longer confidential, if you can no longer rely on the integrity of the data, or if you can no longer count on it being available.

Brainstorm the most damaging scenarios and consider how your stakeholders and messaging may change for each one.

Different scenarios could include:

- Rumors that your campaign has been hacked;
- Credit card and contact information for your donors is stolen;
- Ransomware and an extortion attempt are lodged against your campaign;
- Your systems are wiped and shut down;
- Someone's emails are stolen;

Your adversary steals your administrator's credentials and every file on your campaign drive.

A malicious actor alters statements on your website or public accounts.

Be careful what you say in the present about cyber security 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 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, so that you can draft statements or talking points quickly if an incident occurs. 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.

Questions to include in your Q & A document are:

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.

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

Copyright 2018, President and Fellows of Harvard College

Illustration icons from the Noto Emoji project, licensed under Apache 2.0.