Election Security and Large Counties

Noah Praetz

Abstract State election officials do a tremendous service overseeing and regulating elections in America. But when it comes to defending against cyber threats the work falls to the local election officials—over 8000 nationwide—who mostly control, secure, and run elections. They are on the front lines of this new battlefield. And they are the entities most in need of support and attention from state and federal, public and private partners.

Keywords Elections • Security • Cybersecurity • Local election official
• Support

INTRODUCTION

From my office window I can see The Picasso, a large iron structure, thought to be a woman, by the named sculptor. I would often contemplate problems while watching children and skateboarders play on this centerpiece of Chicago's Daley Plaza. This was the case in June of 2016 when I noticed several emails pop in succession from staff announcing that

N. Praetz (✉)

Cook County Clerk's Office, Chicago, IL, USA

e-mail: noah@praetzconsulting.com

Illinois' statewide voter database was inaccessible. No big deal—it's just maintenance—I thought then. Seemingly, it was an inconsequential occurrence in our state because in Illinois each local election authority has its own voter registration system that shares data “up” to the statewide database. Nearly a month later it was clear that our statewide system had been breached by hackers. Two years later it's been attributed to several Russians working for the Internet Research Agency at the direction of the Kremlin.

Little did I know then that I was a witness to history—at the bleeding edge of an inflection point in the field of election administration. Over the past two years state and local election officials have undergone a tremendous forced maturation process and now the cybersecurity of election systems is the top issue in our field.

And yet, we have significant gaps. Elections are run locally, by county and city bureaucrats dedicated to a free and fair count. They are greatly outmatched against a persistent foreign threat—and the full strength of state and federal resources has yet to reach them. The challenge then, as local election officials, is to quickly understand the fundamental requirements of election security in this era and to pull ourselves up by the bootstraps to meet them.

Elections are the fundamental institution in our country. And, with effort and support, elections will remain strong and resilient, as impervious to external forces as *The Picasso* outside my window.

SUMMARY

Election officials have been securing our nation's votes and voter records for a very long time. They have been securing digital infrastructure for decades. But the changed environment and the expectation of continued sophisticated attacks force them to up their game.

Spurred by the need to defend against foreign enemies, federal and state officials have been working successfully to find a good balance of federal involvement in elections, without trampling on authority that the states zealously guard. Good progress is being made.

State election officials, who protect statewide voter lists everywhere and more systems in some states, and who are often the spokespersons defending our institution, deserve great credit. They provided lead blocking for their locals in the run-up to 2016. And then they provided leadership leading into 2018, first by universally accepting the premise that we are a

target and we are vulnerable, and then by increasingly focusing on supporting locals where most of the risks lie. The Cybersecurity and Infrastructure Security Agency (CISA) charged with providing direct support in this area has also successfully met the continuing demand for information and for services. And the vendors, each of whom are deeply embedded strategic partners to locals, seem to understand the need to be their absolute best.

However, by and large, local election officials are the ones who control, secure, and run elections. Locals—108 offices in Illinois and over 8000 nationwide—are on the front lines of this new battlefield. They control almost the entire election infrastructure. And they are the entities most in need of support and attention. They need help to fortify themselves against the high-probability threat actors they’ve been warned about.

In Cook County, we studied and undertook significant efforts at securing the infrastructure and helping raise awareness within the ecosystem. We concluded that to decrease the likelihood of successful attack on digital services, each election official must have access to an election infrastructure security officer. Most locals don’t have that capacity today.

Local election officials cannot master this problem without direct support of skilled experts. We suggested this be handled by a brigade of digital defenders, or what the United States Department of Homeland Security’s (DHS) Government Coordinating Council (GCC) called “cyber navigators,” supporting local election officials into the future.

These “navigators” should adopt the mantra of Defend, Detect, Recover. They need to accomplish these three vital goals. They can help *improve defenses* within election offices, following the specific recommendations of the Center for Internet Security or Defending Digital Democracy—we believe they can quickly bring up the floor of the elections security ecosystem. They’ll also *establish breach detection techniques*. And they’ll *develop recovery plans* for when attackers penetrate the first and second line.

To accomplish this, the “navigators” will secure free support offered by public and private organizations, like DHS, state governments, and companies like Google, Microsoft, and Cloudflare. They will also work with outside vendors who provide much of the election system infrastructure and support to local officials. Not least, they will build a culture of security that can adapt to evolving threats through training and constant reassessment.

And though election officials appreciate that there was no known successful attack against our infrastructure in 2018, the entire community

remains committed to the security effort because the absence of a successful attack happens to be more a function of our adversaries not engaging than a function of our significant efforts over the last two years.

Voters should feel confident that election officials have resilient systems, with paper ballots and good audits almost everywhere. But voters should also understand that, without continued investment in people and products, the possibility of a successful attack increases as does the likelihood that campaigns may cultivate cynicism about the integrity of our elections for their own purposes. Democracy is not perfect. As Churchill said, “It is the worst form of government except for all the others.” We need to protect it. We will regret it if our democracy is damaged because we looked away at a critical moment.

ELECTION SECURITY POST 2016

When election administrators certify results, they are an essential part of the process that bestows not just power, but legitimacy. And that legitimacy arises because of the essential American belief that our elections reflect a trusted and true accounting of each election. We protect the legitimacy of elections by protecting two virtues, truth and trust, along two fronts, infrastructure and information. By and large, truth can be protected with policies and tools that can ensure a fair and accurate count. We protect trust by continuing to deliver election services as expected by our voters.

Since 2000 the Cook County Election Division has tried to lead on technology and security—using applied forensics in elections, creating widely circulated cybersecurity checklists in advance of the 2016 elections, and publishing the first White Paper written by election officials in the wake of the 2016 attacks. In 2017 Cook County helped the Center for Internet Security (CIS) adapt their digital security expertise to the unique context of elections and spent some time talking to the Defending Digital Democracy (DDD) program at Harvard’s Belfer Center for Science and International Affairs. I was chosen as co-chair of the Government Coordinating Council that the Department of Homeland Security created to help address election security. In that effort we worked with federal, state, and local leaders in elections, technology, intelligence, and law enforcement.

There are two truths that need to dominate the narrative:

- The threats to election infrastructure are real.
- Elections are largely run and secured locally, so security efforts and investments need to be concentrated locally; but those efforts need to be supported by the federal government and led by the states.

As election officials, we had to accept the conclusion of the intelligence community—our elections were attacked. And while enemy efforts using social media, news, and influence systems were more successful in 2016 than those directed at election infrastructure, we expect the attacks will evolve. It is important to recognize that attacks in the information sphere are important and do affect trust in the institution, and election officials have little control in that space. Instead, election administrators must defend their section of the line where they have almost complete control—by securing all elements of our voting infrastructure.

CYBERSECURITY—ONE MORE SWORD TO JUGGLE

Prior to 2000, election administrators served mostly as wedding planners, making sure the right list of people came together in the right place with the right stuff. After *Bush v. Gore*, the 2002 Help America Vote Act (HAVA) heralded in a new era of voting technology, and we became legal compliance and IT managers. We’ve been working to protect an expanding digital technology footprint since then. But the 2016 election showed irrefutably that sophisticated attacks are to be expected and that we must also be cybersecurity managers.

Foreign governments, foreign non-state actors, and domestic troublemakers have the capacity and desire to corrode the essential public belief that our election outcomes are true and reliable. To very different degrees, this threat applies to both preliminary results announced on election night and official, final results. Beyond corrupting election results, the threat also reaches the large variety of systems used to run seamless elections.

Therefore, the new security mantra, or security framework, for local election officials must be “defend, detect, recover.”

Security isn’t just about defense. Perfect defense is difficult or even impossible. Our best resourced companies like Uber, Equifax, HBO, and Sony and government entities like the Federal Office of Personnel Management and the Illinois State Board of Elections have been breached despite significant defensive investments. Instead, the challenge of security

is to ensure that no successful attack exceeds our resilience—our ability to detect and recover, whether that requires restoring lost data or even recounting ballots—to establish election results that are trusted and true.

Because state laws vary, local election officials confront a different security matrix in each state, which affects their ability to defend, detect, and/or recover. States with great audit processes (detection) and paper ballots (recovery) are much more resilient by definition; and the burden of defending their voting system perfectly is consequently much lower. On the other hand, states without great audits and without paper ballots place the unenviable burden of perfect defense on their local election administrators.

In 2017, Cook County Clerk David Orr and I published a White Paper called “2020 Vision: Election Security in the Age of Committed Foreign Threats.” We published it to help guide policy makers and election officials in their actions post 2016. Our key recommendations are included at the end of the chapter.

ELECTIONS ARE SECURED LOCALLY

State election officials deserve respect for their responsibilities and efforts. They are often the mouthpiece of our institution and responsible for managing the regulatory framework. For the past 16 years, many have also managed their state’s voter registration systems. In some states they take a far more active role in protecting other parts of the infrastructure. And in 2016, states rather than local jurisdictions were the named targets. But let there be no mistake—local election officials are on the front lines of this new battle field. So, by and large, local election offices secure the nation’s election infrastructure. Locals install, store, monitor, test, deploy, run, and audit the voting machines and software. Locals install, store, monitor, test, deploy, run, and audit the electronic pollbooks. It is locals who manage warehouses, informational websites, voter databases, polling places, GIS systems, results reporting systems, military voting systems, command centers, and the myriad digital services we rely upon in modern American elections. It is a local job to defend these systems, to institute controls that would detect breach, and to deploy mitigation strategies that can guarantee election processes and results that are trusted and true. It is their job to ensure recovery.

Most are county officers, and are facing down powerful, shadowy adversaries, much like Andy of Mayberry sent to repel an invading army. They need advice, support, and resources—first, for better technology and

routine hand-counted audits which can give additional confidence that digital results are accurate. Second, and most critically, there is a pressing need for top-notch personnel with the skills to navigate the current cyber battlefield. Our country's local election officials need direct human support as they work to defend the institution against the onslaught of digital threats they've been warned about.

COOK COUNTY EFFORTS

Since the summer of 2016, in Cook County we stepped up our efforts to protect ourselves and to protect the broader ecosystem.

We introduced additional hand-counted audits to our state-mandated 5 percent machine retabulation. And we pushed state legislation to add additional audits to election results—in the form of risk limiting audits.

We did a comprehensive mapping of all our systems and conducted a point and line analysis of potential vulnerabilities. We documented all defensive measures employed and created a list of those we hoped to employ going forward. We also documented all methods of detecting breach, as well as those we hoped to employ in the future. Finally, we developed our recovery plans for any breach at any point on any system. And in 2018 and 2019 the office will practice every recovery method.

We procured new election equipment that will be easier to defend and will make detection and recovery significantly easier.

We introduced state legislation to help local election officials bring in more expertise and cyber monitoring capability.

We worked to create a communication structure in Illinois with federal, state, and local cyber experts, technology experts, law enforcement officials, and election officials.

We teamed with our neighbors at the Chicago Board of Elections to hire an election infrastructure and information security officer.

We worked with MS-ISAC (the Multi-State Information Sharing and Analysis Center) to get rapid intelligence on vulnerabilities and specific threat information to our networks. And we have pushed our colleagues around the state to join it and the elections ISAC. Additionally, we have gotten threat briefings from the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI).

We worked with DHS to conduct cyber scans of our websites and to run a full risk and vulnerability assessment. And let me say that I am glad the folks working for Homeland Security are on our team. I firmly believe if every election official, state or local, undertook a similar effort, there

would be a deafening roar from my colleagues for more resources to procure modern technology and more talented people to institute modern controls.

We worked with the folks at DEF CON® on some of their activities related to training election officials on the defense of networks. DEF CON®, held annually in Las Vegas, Nevada, is one of the world's largest hacker conventions. Primary attendees include computer security professionals, security researchers, and other hackers with a general interest in security. Government employees, corporate professionals, and journalists are often in attendance

I co-chaired the newly created Government Coordinating Council set up with DHS to help drive federal policy and resource allocation. On the GCC, I sit alongside the Chairman of the Election Assistance Commission (EAC), the President of the National Association of Secretaries of State (NASS), the President of the National Association of State Election Directors (NASED), and from the DHS Deputy Assistant Secretary, Infrastructure Protection, National Protection and Programs Directorate (NPPD). As one of nine designated representatives of local election officials, I tried to continually push for the advancement of the concerns of local officials.

And in all these efforts we have learned that coordinating efforts is critical to our individual and ecosystem success.

COORDINATED EFFORTS

There has been a tremendous amount of attention on the states, and their relationship to the federal government and it's been good to see that relationship mending and great information starting to be shared between the two groups. On the GCC we worked hard to refine a plan for securing our sector as well as protocols for sharing information throughout the ecosystem. We worked with the private sector vendor community to ensure we had a common approach to protecting the sector.

DHS now knows how to communicate with the state-level election professionals and vice versa. What remains unfulfilled is the assurance that the information can get all the way down to the local level and that the locals are prepared to digest the information and take necessary action.

It is time to ensure that the successful effort to normalize relations with state officials be duplicated with local election officials. Like an iceberg, the mass, and indeed most of the risks to the nation's election infrastruc-

ture, lies below the surface. And its security lies in the hands of women and men who run elections at the local level.

Given our federalist system, the path for successfully fortifying local election officials is through state government and state election officials. But it's important that they envision their job as helping ensure locals are resourced appropriately and meeting important security metrics. I have no doubt that our state officials are up for the challenge and I look forward to assisting our industry mature in this direction quickly.

INCREASED STABLE INVESTMENT AND SHORT-TERM SPENDING

Locals look to state and federal funders and regulators to fortify them on this battlefield. Given the costs of regular technology refreshes and support for human resources with cyber capacity, the needed investment is very large, perhaps on the order of HAVA 2.0.¹ And state and local election officials need a signal that they can invest now for security and not have to squirrel away recent money for some future episode.

Nevertheless, the 2018 investment was greatly appreciated. Congress released \$380 million to combat the election cybersecurity threat. And that is an important start. It may be necessary to invest that much annually. Meanwhile, Americans justifiably concerned about the costs need confidence that this money will be spent well.

In my mind there are two top priorities. First, a handful of states and counties still have paperless voting systems. These must be replaced as soon as possible. Second, everywhere, we must improve the security capacities of local election offices. Most are run by just a handful of incredibly dedicated and hardworking heroes. But a handful of people making critical security decisions are outmatched against the threats we've been warned about.

In 2018 in a Chicago newspaper former Cook County Clerk David Orr and I called for a brigade of digital defenders to be deployed to serve election offices around Illinois and the nation, working through the 2020 presidential election and beyond. Later that year, the GCC, comprising the leadership of America's election organizations, suggested a similar construct, suggesting that states employ "cyber navigators" to help fortify local election officials.

¹HAVA 2.0 refers to the Consolidated Appropriations Act of 2018 which included \$380 million in grants, made available to states to improve the administration of elections for federal office, including to enhance technology and make certain election security improvements. The grants are often referred to as HAVA 2.0 or the 2018 HAVA Election Security Fund.

ILLINOIS APPROACH

The Illinois approach illustrates the value of collaboration and how time-intensive this process will be. In Illinois we formulated a loose security group consisting of representatives of DHS, FBI, the Illinois State Police and their Cyber Team, Illinois Information Security Office, the leadership of the local election official associations, and the State Board of Elections. Originally some local officials and the State Board of Elections had desired to pass through the HAVA funds to the local election officials based largely upon voting age population. But as our group and state legislators digested the cybersecurity problem, we recognized that such a distribution would not be effective enough in fortifying most of the locals. First, regardless of the number of voters served, all 108 election officials had nearly identical cyber footprints, in that they had the same number of networked-attached digitally exposed systems, websites, voting systems, e-pollbooks, command centers, voter registration systems, and so on. Second, the larger offices already had some capacity to tackle this problem—whereas the smaller offices were squeezed so tightly they could barely comply with the current requirements, let alone secure the entire elections threat surface area.

After the GCC issued guidance suggesting “cyber navigators,” the state legislature mandated that at least one-half of the 2018 HAVA funds just released be expended on a “cyber navigator” program to be administered by the State Board of Elections. The State Board is getting help fulfilling this mandate from other organizations with cyber expertise. By and large, local election officials supported the bill. And our State Board is eminently capable of fulfilling the mandate.

These “navigators” need to accomplish three vital goals. First, they should work to institute the election security framework—defend, detect, recover. They can help improve defenses within election offices, following the specific recommendations of CIS. They’ll quickly bring up the floor of the election security ecosystem. Appropriately supported, we can see massive improvement very quickly. There is low-hanging fruit, but even low-hanging fruit needs to be plucked. They’ll also work to support locals’ efforts at instituting detection techniques and recovery plans. Second, the “navigators” will do the work necessary to secure the free support being offered by public and private organizations, like DHS, state resources, Microsoft, Google, and Cloudflare, or the Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC); they will also work with the outside vendors who provide much of the election infrastructure

and support to local officials. More importantly, they will help build a culture of security that adapts to the evolving threats we face through training and constant assessment efforts. Illinois' 108 local election offices will mature quickly with this reinforcement. As specific mitigations and upgrades are identified by navigators, the State Board should be positioned to quickly provide that investment.

The State Board of Elections will take some portion of the remainder of the HAVA funds to support their own infrastructure, naturally, since they manage and maintain the statewide voter database. Some portion of the remainder is and will be distributed to the local election officials to invest as they see fit, subject to the guidelines. The state legislature sought to compel participation in the navigator program by making receipt of future grants contingent upon local official participation.

In Illinois, we recognized that this is inherently a local problem. But we also recognize that locals cannot solve this problem themselves. This coordinated, managed approach assures appropriate assessment and remediation efforts can be efficiently implemented. Officials are utilizing existing expertise from other areas of federal, state, and local government as force multipliers.

This massive reinforcement effort can be accomplished nationwide. And it can be done now. It will require the states to cut through the red tape that can delay action. This may mean relying on existing contracts, or even emergency procurements. But states should do whatever they need to do to get the army of "navigators" on the ground as quickly as possible. After all, the danger is not hypothetical. Election officials are bracing against the renewed attacks they've been told to expect.

SUPPORTING A RESILIENT PUBLIC

One job of an election administrator is to conduct elections properly so that losing candidates accept the fact that they lost fairly. Anything that hinders their ability to do that decreases confidence in the system, and undermines their ability to bestow legitimacy—not just victory.

Election officials deploy a variety of networked connected digital services, such as voter registration systems, and unofficial election results displays. Each of these is a ripe target for our adversaries. A successful attack against those services may not change a single vote, but could still damage public confidence. This is particularly true in a time of great public suspicion, exacerbated by a disappointing proliferation of gracelessness and grandstanding.

Our public confidence is already weaker than it should be. Vacillating voting rights rules, no matter how marginal the effect, are disconcerting to many people, naturally suspect given our history. Additionally, some media, activist groups, and politicians have acted in ways that ultimately prey on Americans' insecurities about their most cherished institution, either through wildly outlandish claims of fraud or through claims of suppression that are sometimes exaggerated. Such actions do hinder election officials' ability to bestow not just victory, but legitimacy. We must be very careful to calculate not just the relative effects on power that election rule changes can have, but also the relative effects on legitimacy. Or put another way—will losers be more or less likely to accept that they lost fairly.

Some losing candidates are already apt to call their defeats into doubt. A new digital breach—no matter how far removed from the vote counting system—could turn sore losers to cynicism, disbelief, even revolt. That's the reaction the enemies of the United States want.

In fact, in the face of direct targeting of a state or local election office it is very possible that there will be some service disruptions—most likely to the network connected digital services like election results websites.

The bottom line is we can't eliminate every chance of breach, but we can make sure that successful attacks are rare. And we can provide assurances that we are prepared to recover quickly when they happen. We can do this with support at the local level.

As Americans, we get to choose how we want to respond to potential disruptions. The damage of a foreign attack on our elections infrastructure will be greatly diminished if the targeted institution is also being supported internally with respect.

EXHIBIT 1: SPECIFIC SUGGESTIONS FROM COOK COUNTY WHITE PAPER—DECEMBER 2017

Responsibilities of Policymakers and Funders

Defend

Increase the defensive capacity of local and state election officials by:

1. Supporting a digital network for all local election officials that will *facilitate rapid sharing of threats and incidents*, as well as *supporting increased training and resiliency*,

2. *Financing an Election Infrastructure and Information Security Officer (EIISO)* (or consultant) servicing every local and state election official in the country;
3. *Ensuring that threat and incident information known to Government is shared* appropriately throughout the election ecosystem.

Detect

Increase the catastrophic breach detection capacity by *incentivizing*:

1. The use of *modern public audits* of all elections;
2. The use of *modern voting technology* that captures a digital image of each ballot that can be tied to the original ballot and the cast ballot record;
3. The use of *monitoring sensors on the networks of all* willing election officials.

Recover

Eliminate even the most remote possibility of an undetectable catastrophic breach by *replacing all paperless voting systems* that currently serve nearly 20 percent of the country.

Release election officials from their burden of being perfect every single time!

Potential Approach for Election Officials and Their Election Infrastructure and Information Security Officer:

Defend

- *Get experts* into the office. Engage outside cybersecurity resources and professionals. No election offices can handle this problem on their own. Inside most elections offices, there simply is not the complete capacity to accept the threat, assess the vulnerability, digest recommendations, manage mitigations, and perfect recovery.
 - Utilize as many free local, state, and federal (DHS, CIS, and MS-ISAC) tools as possible,
If government resources are unavailable, or underwhelming, hire private firms or partner with academic institutions.
 - Collaborate with the local, state, and federal government because we are not alone in facing this type of threat include the fusion centers.

- Bring in outside resources to partner with information technology and information security teams, with a focus solely on election security.

The reality is that most election officials share their internal information technology and security resources with every other county office engaged in critical activities, such as health and public safety. It can be nearly impossible to get the attention necessary for election security unless it is the primary focus of those resources.

- Understand and *limit the threat surface area*; or all possible points of vulnerability for malicious attack.
 - Inventory all election related systems including the: voting machine and vote counting system; e-pollbook system; voter registration/election management system; mail ballot delivery and processing system; and online systems such as voter registration, mail ballot request tools, voter information lookup;
 - Map how systems work and data flows, and mark every single point of vulnerability;
 - Limit the threat surface area by making policy decisions that reduce points of vulnerability wherever possible (this is about managing risk, not eliminating it).
- *Employ defense tactics* and policies for each system—online or not:
 - Implement the Center for Internet Security’s top 20 cyber controls. Do the top five first. These include:
 - 1 Inventory of Authorized and Unauthorized Devices
 - 2 Inventory of Authorized and Unauthorized Software
 - 3 Secure Configurations for Hardware and Software
 - 4 Continuous Vulnerability Assessment and Remediation
 - 5 Controlled Use of Administrative Privileges
 - 6 Maintenance, Monitoring, and Analysis of Audit Logs
 - 7 Email and Web Browser Protections
 - 8 Malware Defenses
 - 9 Limitation and Control of Network Ports
 - 10 Data Recovery Capability
 - 11 Secure Configurations for Network Devices
 - 12 Boundary Defense
 - 13 Data Protection

- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control
- 17 Security Skills Assessment and Appropriate Training to Fill Gaps
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises
- Employ election system-specific defense and detection tactics across specific systems:
- These can include all the hardening options that systems may have, such as locks, seals, chain of custody, advanced authentication, and so on.

Detect

- **Inventory of Authorized and Unauthorized Devices** For each vulnerability point identified in the mapping process, *consider a method of detecting* whether something anomalous has happened; or brainstorm the first place such an intrusion might be detectable.
- *Validate everything*; every available log should be checked including seals, time sheets, cameras, swipe cards, login data, registration statistics, and so on.
 - Behavioral analysis tools and procedures can and will point out what is going on. For example, voter registration follows a natural pattern year over year. Identifying the pattern and watching for anomalous behavior works.
- *Use forensics* when possible.
 - A forensics analysis of the software system employed can offer a high level of confidence that it is operating as certified. This is particularly true in the voting system environment. Comparing snapshots of deployed software with a clean reference copy during a live election is a powerful verification technique.
- *Conduct public audits* of the election results that allow for a visual comparison of the cast ballot record with the ballot itself.
 - Be transparent and brace for public scrutiny.
 - Crowdsourcing the election brings the greatest confidence, but also the greatest public scrutiny. “Sausage making” will be on full display. Consider publishing ballot images scrubbed of identifying marks. In the short run this can create volatility, and people may

scrutinize the office and the software used, but ultimately the confidence levels will be increased.

- Work to investigate audit styles that bring the highest level of confidence to the most stakeholders. Consider the use of sophisticated yet efficient testing algorithms, such as risk limiting audits.

Recover

- For each vulnerability point, *assume a successful breach and determine how to recover*.
- Where possible, make policy decisions and investments that yield the clearest *path to recovery*.
 - For example, on electronic voting machines: after removing paperless systems consider that ballot marking devices are better than machines with paper audit trails. Digital scanning devices that create images of ballots are better than scanning devices that don't.
- Build in *redundancy that doesn't rely on technology*.
 - For example, paper pollbooks back up electronic pollbooks. Emergency paper ballots back up corrupted (or just malfunctioning) touch-screen or ballot marking devices.
- *Practice recovery* with professional staff, advisors, and vendors by running drills and exercises. Theory is only theory. Practice makes it real.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.