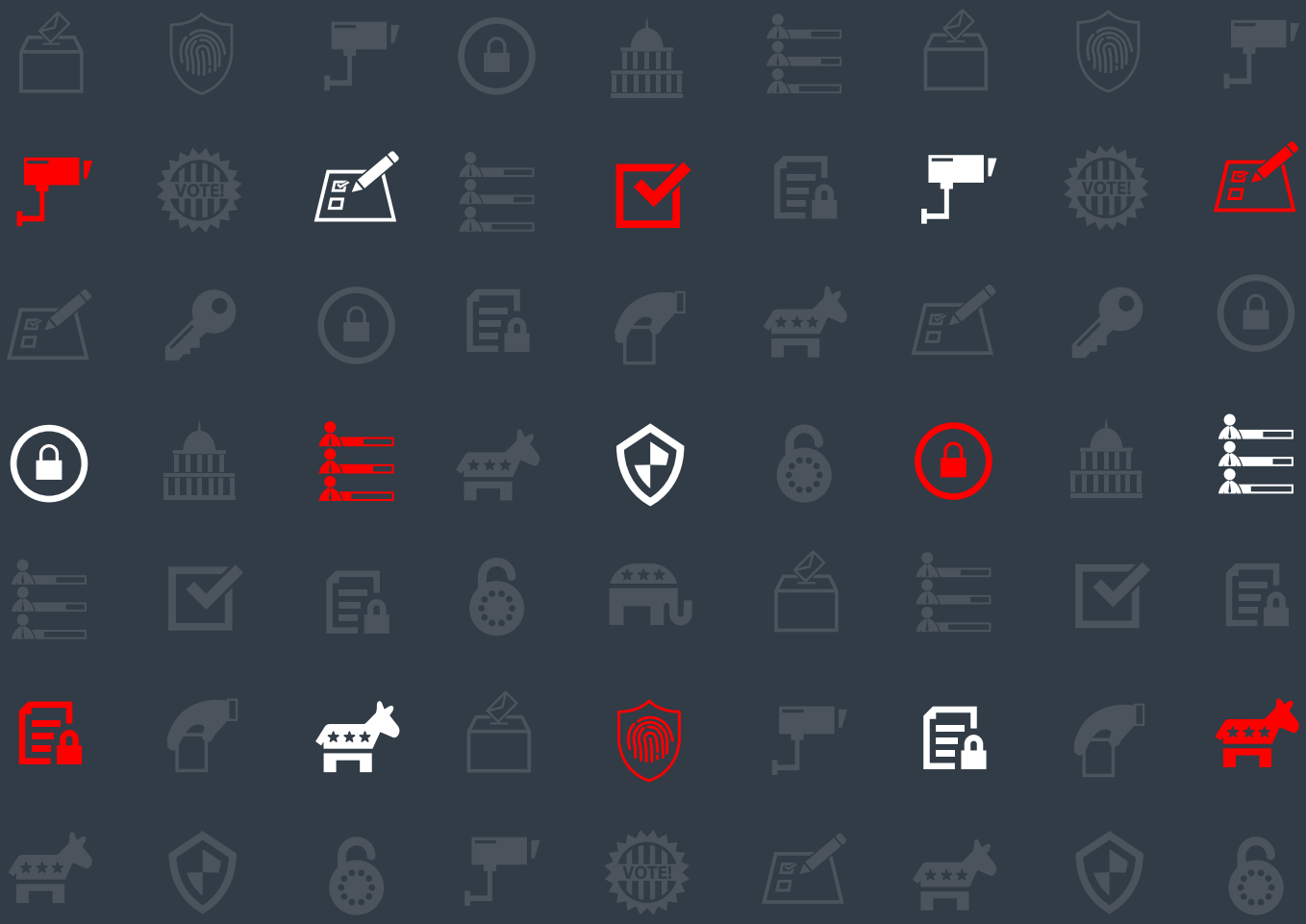
CARBON BLACK

DEMOCRACY AT RISK

More than 15 million voters may stay home on Election Day over cyber-security doubts



EXECUTIVE SUMMARY

Election security and the use of electronic voting machines have, for the last decade, been divisive issues in the United States. Following the 2000 election (Bush vs. Gore), researchers from academia and the private sector have demonstrated how vulnerable the election system may be to cyber attack.

Among some of the vulnerabilities revealed have been:

- The ease of which electronic voting machines can be manipulated to **alter votes.**
- The ability to **compromise** voter-registration databases.
- The prospect that voting systems and process can be shut down, delayed or restricted.

To date, there have been no indications that technology in previous elections has been tampered with. However, in the wake of these concerns and recent hacks against the Democratic National Committee, the Democratic Congressional Campaign Committee and election databases, it is becoming clear that tampering with an election is a very real possibility. That potential for tampering, and overall doubts about election security, may play a role in keeping voters home on Election Day.

In September 2016, Carbon Black conducted an online survey of 700 voters in the United States to understand how aware the electorate is of the security risks associated with electronic voting machines, measure possible doubt that these risks have cast over elections and voter turnout, and ultimately, increase awareness around security concerns to help drive change.

Among the results from the survey, we found:

- **More than half of U.S. voters (56%) are concerned** that this year's election will be affected by hacking/cyber attack.
- **More than half of U.S. voters (58%)** said it's likely electronic voting machines could be hacked during the election.
- **More than one-third of voters (36%)** feel their voting information is insecure.
- **1 out of every 5 voters** who said their voting information is insecure will consider not voting in this year's election given their concerns - amounting to **more than 15 million voters** potentially staying away from the polls over cyber-security concerns.
- Voters believe a **U.S. insider threat (28%), Russia (17%) and the candidates themselves (15%) pose the biggest risks** when it comes to hacking the 2016 election.

Specific vulnerabilities on electronic voting machines and the election system have been public for years, and the prevailing sentiment among voters that the 2016 election may not be safe from cyber attacks adds an additional, clarion call that stricter security standards are needed to instill trust. If voters lose trust in the voting process, our democracy may be at risk.

This report ties data found in our survey to the ubiquity of electronic voting machines in the United States to determine if the doubt voters are experiencing is warranted.

This report also includes several security recommendations that may be used to better protect voting data and, ultimately, our democracy. Recommendations focus on hardening, auditing, and transparency to establish public trust and create processes to verify the integrity of the system.

Fundamentally, the strongest recommendation for electronic voting machines is to treat them as fixed-function devices that perform a single function, versus having fully-functioning computers that can be more vulnerable to manipulation. Mitigating risk also includes supply-chain risk. Many of our government processes, including elections, rely on digital systems that must be adequately secured at each stage in the process.

> IF VOTERS LOSE TRUST IN THE VOTING PROCESS, OUR DEMOCRACY MAY BE AT RISK.

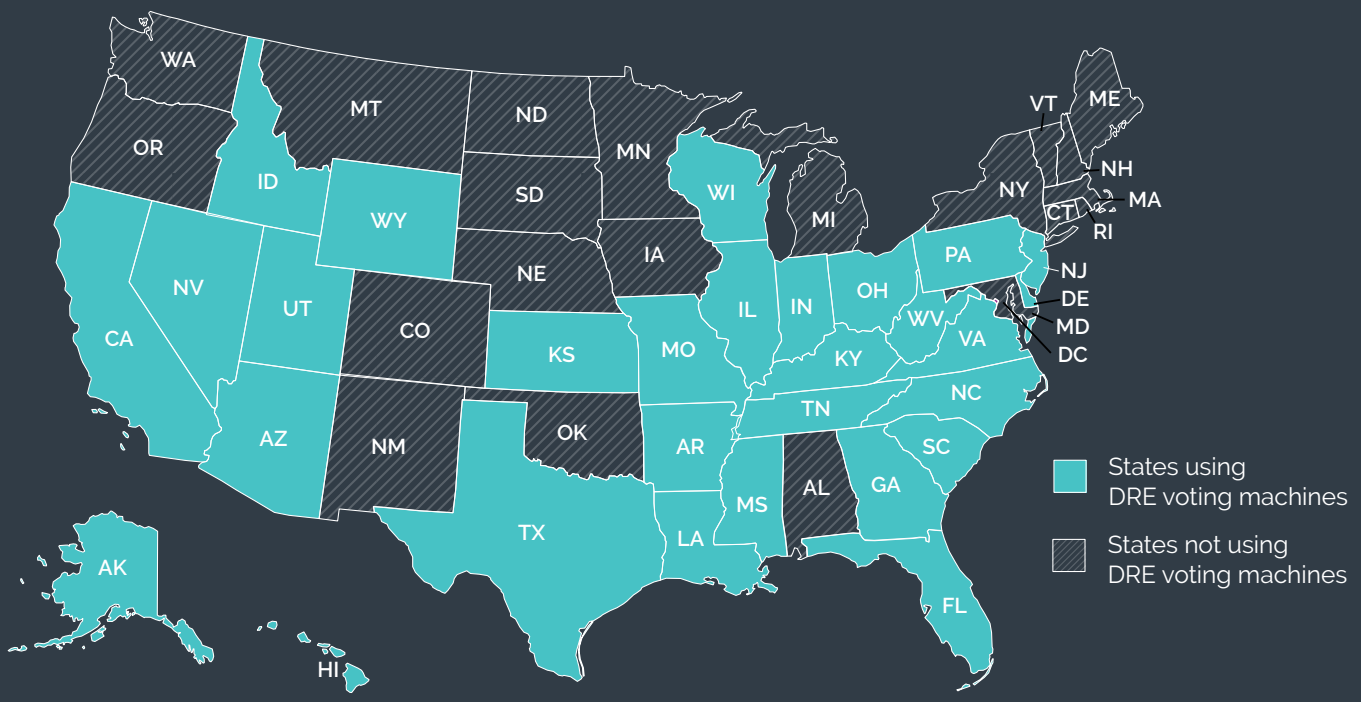
ELECTRONIC VOTING MACHINES AT RISK IN THE UNITED STATES

This year, about 25% of the United States (representing approximately 55 million voters) will use electronic voting machines on November 8 to elect the next president.

Overall, various types and brands of electronic voting machines will be used throughout the United States in the 2016 election. The type of machine considered to be the most vulnerable to attack is the "direct-recording electronic" (DRE) machine. Many of these machines are running severely outdated operated systems such as Windows XP, which has not been patched by Microsoft since April 2014.

The map below from **Verified Voting**, a group dedicated to improving election-system integrity, shows which states will use DREs on Election Day.

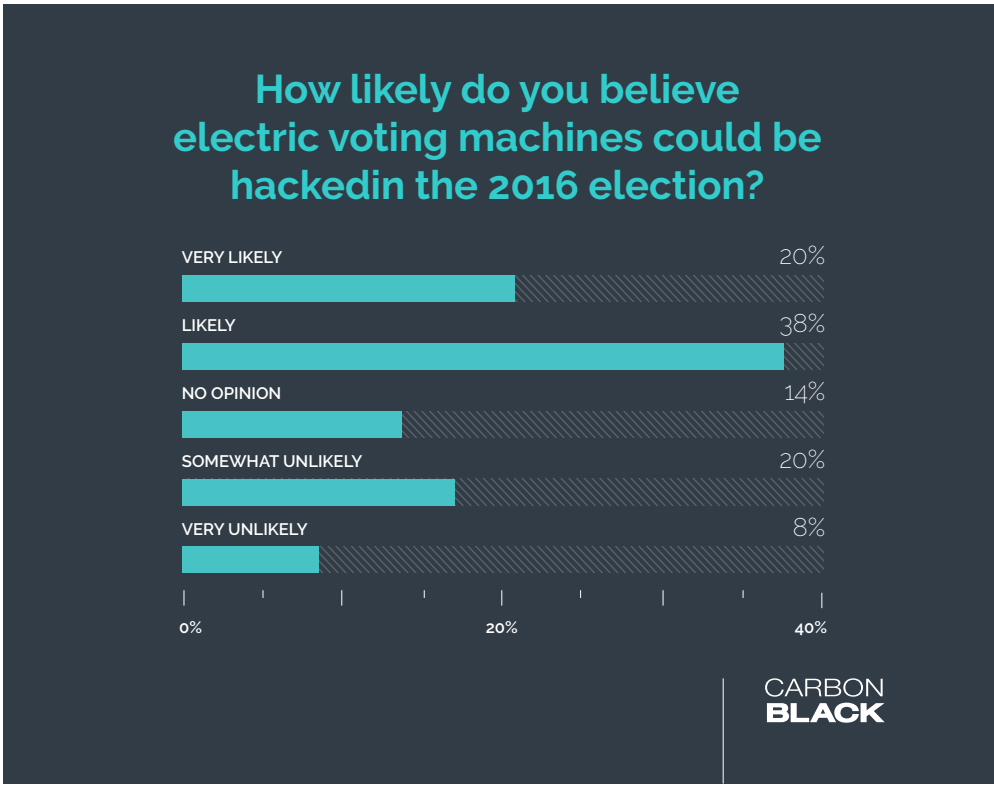
States using DRE voting machines in the 2016 election (DREs are considered the most vulnerable machines)



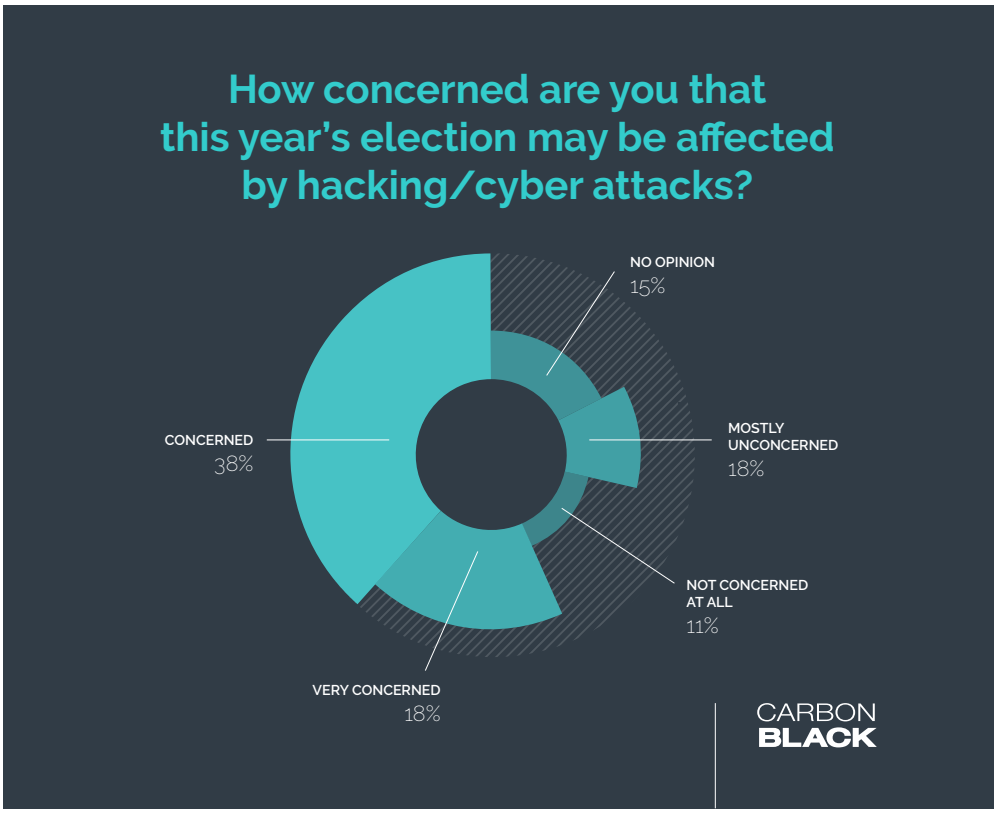
*Map data from verifiedvoting.org

CARBON BLACK

The security vulnerabilities in electronic voting machines are not lost on voters. In our survey, **58% of voters said it is "likely" or "very likely" that electronic voting machines could be hacked in the 2016 election.**



It's clear that our electorate is very aware of the problem, when we asked: "How concerned are you that this year's election may be affected by hacking/cyber attacks?" **More than half of voters (56%) said they are "concerned" or "very concerned."**



36%

OF VOTERS FEEL THEIR VOTING INFORMATION IS INSECURE

1/5 = 15m

1/5 OF VOTERS ARE CONSIDERING NOT VOTING, RESULTING IN MORE THAN 15 MILLION VOTERS AT HOME ON ELECTION DAY

CARBON BLACK

Further doubt crept into voters' consciousness when they were asked: "How secure do you feel your voting information is for this year's election?" **More than one-third of voters (36%) said they felt their voting information is either "somewhat insecure" or "very insecure." Only 12% of voters said they felt their voting information is "very secure."**

DOUBT ON ELECTION DAY

That doubt, if tied to voter inaction, poses a true risk to our democracy. **1 in 5 voters** who felt "somewhat insecure" or "very insecure" about their voting information said they **would consider not voting** in this year's election given their cyber-security concerns.

With approximately 218,000,000 voters in the United States, that insecurity may leave **more than 15,000,000 voters home from the polls on Election Day.**

There are a few silver linings here, though. First, to date, there has been no indication that previous elections have been tampered with. The second, possible silver lining, is that some states that use electronic voting machines tether the machines to a voter-verified paper audit trail (VVPAT), which allows voters to verify that their vote was cast correctly and detect possible election fraud.

While a VVPAT is not immune to all types of fraud, it serves as an additional security layer for districts to assuage voters that their votes are being cast accurately. According to **Verified Voting**, "well-designed and properly performed post-election audits can significantly mitigate the threat of error, and should be considered integral to any vote counting system." A VVPAT helps empower the voting districts to conduct such audits.

About half of states have a "meaningful" post-election audit, **according to Verified Voting**.

ELECTRONIC VOTING MACHINES IN KEY BATTLEGROUND STATES

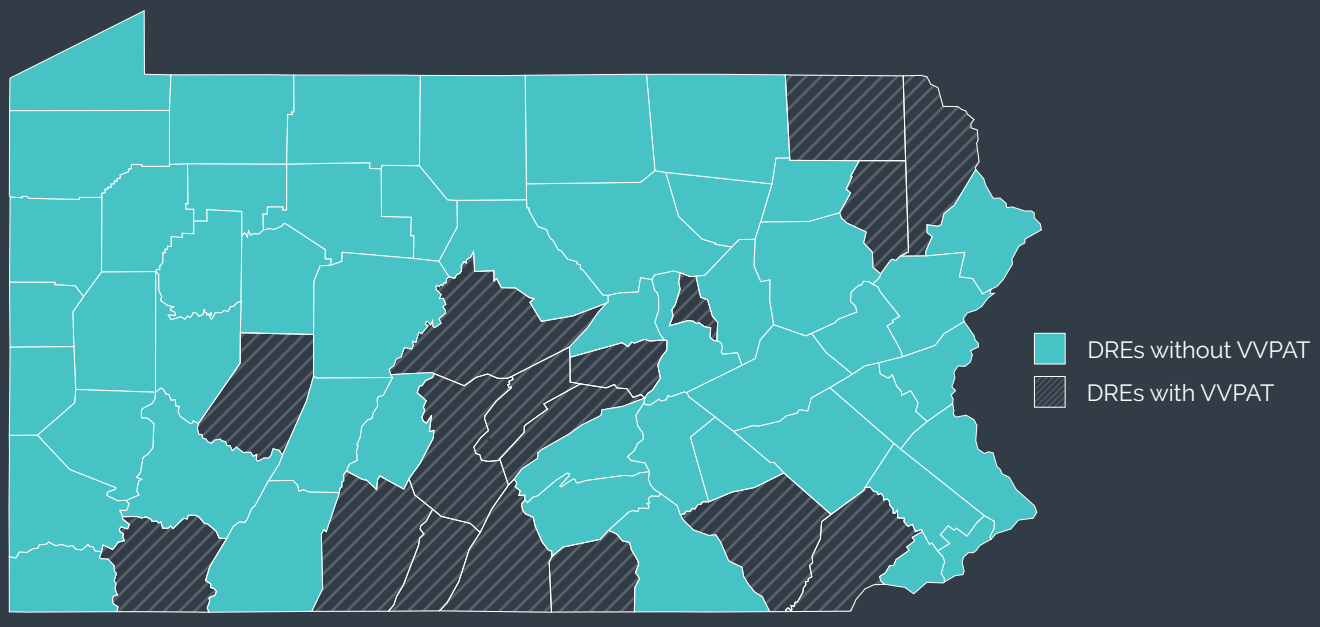
Pennsylvania, largely thought to be a key battleground state in the upcoming election, may be the largest concern when it comes to electronic voting machines, given the ubiquity of DRE machines with no VVPAT. The graphic below from Verified Voting shows a county-by-county breakdown of how prevalent DREs without a paper trail are in Pennsylvania.

According to **Verified Voting**, "it is crucial that voting equipment provide or require the use of a permanent record of each vote that can be checked for accuracy by the voter before the vote is submitted, and is difficult or impossible to alter after it has been checked. Many of the Direct Recording Electronic (DRE) systems used in the U.S. do not satisfy this requirement."

Conversely, Florida and Ohio (also key battleground states that use electronic voting machines) may be considered relatively "safer." Ohio conducts post-election audits and also has a manual recount provision that kicks in for close races. Florida also has an audit requirement. Both will use DRE machines in the upcoming election.

It is worth repeating that there has been no official record of election tampering to date. However, based on our survey, the evident danger of electronic voting lies in the **suspicion of tampering**. Without a systematic approach to keeping systems and votes secure, as well a repeatable and trustworthy audit system, doubt will inevitably creep into voters' consciousness.

Pennsylvania Counties Using DRE MACHINES without Voter Verified Paper Audit Trails (VVPAT)



*Map data from verifiedvoting.org

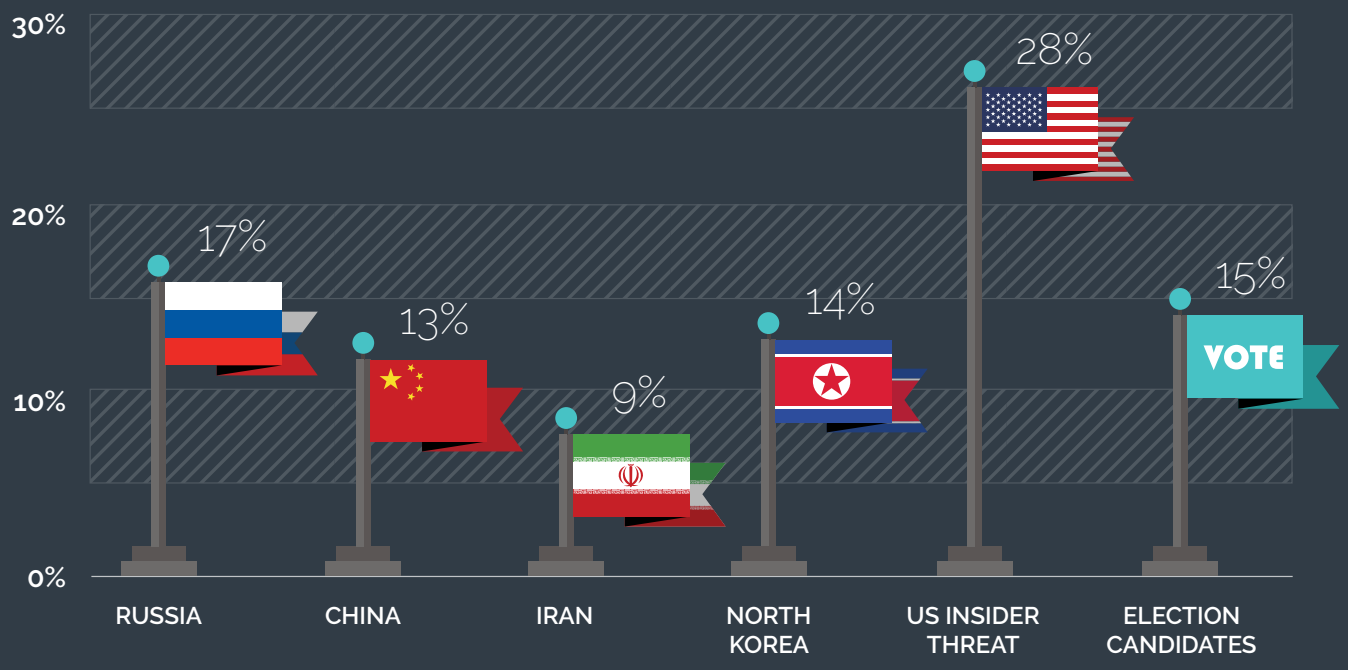
BIGGEST PERCEIVED THREATS

#1 U.S. INSIDER THREAT (28%)
#2 RUSSIA (17%)
#3 ELECTION CANDIDATES (15%)

Voters have not had a shortage of recent news coverage regarding a "hacked election." Leaked emails/voter information, potential Russian influence in the election, and insecure electronic voting machines have all crept into voters' consciousness of late. Our survey results reflect these sentiments.

The graphic below shows the survey results to the question: "Which entities do you think pose the biggest potential risk when it comes to hacking the 2016 election?"

Which entities do you think pose the biggest potential risk when it comes to hacking the 2016 election?



*approximately 4% replied 'other'

SECURITY RECOMMENDATIONS

While there are plenty of risks and doubt, as confirmed by the research, there are paths forward to help mitigate risks and re-establish trust with voters around the use of electronic voting machines. Most importantly, our leaders and the manufacturers of these voting machines need to be reminded that they are computers - very powerful machines. In today's connected world, computers can easily be manipulated without the proper security measures.

Security concerns are not solely about an attacker compromising individual voting machines. They also include supply-chain risk. Many of our government processes rely on digital systems. At any point during election processes, an attacker can find a weakness and potentially change a vote, modify the party that the candidates represent, and more. Our failure to secure these digital systems is placing our democracy at risk. We must consider the vulnerabilities at every stage: from the parts used in the manufacturing of electronic voting machines, to their manufacturing, delivery, storage, operation, and verification.

HARDENED MACHINES, SYSTEMS AND PROCESSES WITH CONTINUOUS MONITORING

Electronic voting machines should be fixed-function, single-use devices. They should not have the capability to run new applications, connect to the Internet, or install updates. If the underlying operating system allows for different applications to execute, security software that prevents this and enforces policies must be used. Additionally, continuous monitoring of the operation and health of machines, systems and databases needs to occur, as well as the inspection of what is occurring on the systems and what is being transmitted in order to look for anomalies. Voting machines should be given to non-partisan review boards to analyze and ensure that they were not tampered with and function as expected.

VERIFIABLE PAPER AUDIT TRAIL / TRANSPARENCY

All electronic voting machines and processes must have a verifiable paper trail that should be fully auditable, both with operations (i.e. placing and tallying of votes) and of the underlying software and hardware components used. The types of machines, the versions, the vendors, and vendor political affiliations and contributions should be publicly posted in polling stations. Where applicable, alternatives to electronic voting should be provided at each polling station. Legislation should continue to pursue the safest alternatives to electronic voting.

ENCRYPTION

Encryption of the database and tallied results should occur with a central commission holding the decryption keys. There should be auditing of transmission and decryption of the results, maintaining a forensically sound chain of custody.

NETWORK ISOLATION

There should be no network connectivity for any voting machine. If the system must be connected to other devices or the Internet, it should be a single, always-on virtual private network that routes all communications through a central hub over an encrypted connection.

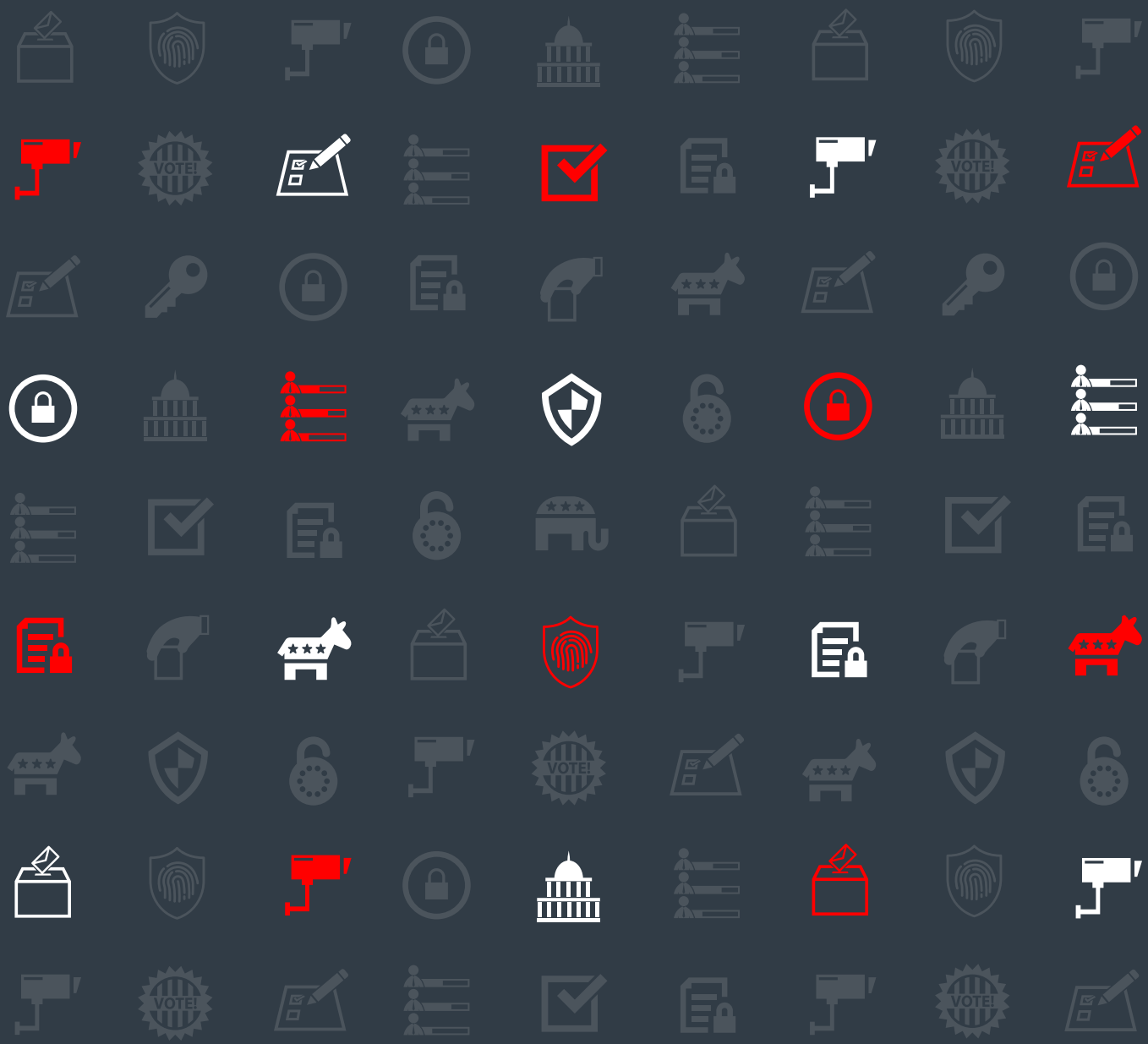
CARBON BLACK

METHODOLOGY

In September 2016, Carbon Black conducted an online survey of 700 registered voters in the United States to determine their sentiments regarding election security and the security of electronic voting machines. Respondents ranged in age from 18-54. "More than 15 million voters" noted as staying home on Election Day in the report was extrapolated from the approximate number of voters in the United States (218,000,000), combined with our survey results.

ABOUT

Carbon Black has designed the most complete next-gen endpoint-security platform, enabling organizations to stop the most attacks, see every threat, close security gaps, and evolve their defenses. The Cb Endpoint Security Platform helps organizations of all sizes replace legacy antivirus technology, lock down systems, and arm incident response teams with advanced tools to proactively hunt down threats. Today, Carbon Black has approximately 2,000 worldwide customers, including 25 of the Fortune 100 and more than 600 employees. Carbon Black was voted Best Endpoint Protection by security professionals in the SANS Institute's Best of 2015 Awards.



CARBON
BLACK

1100 Winter Street
Waltham, MA 02451
P: 617.393.7400
F: 617.393.7499

carbonblack.com