THE NEW CENTER

Policy Paper

Think Centered

Cybersecuring America

CAN WE STAY AHEAD OF THE HACKERS?

Cybersecuring America

CAN WE STAY AHEAD OF THE HACKERS?

March 2020

AUTHOR

Laurin Schwab

Policy Analyst

laurin@newcenter.org

ABOUT THE NEW CENTER

American politics is broken, with the far left and far right making it increasingly impossible to govern. This will not change until a vibrant center emerges with an agenda that appeals to the vast majority of the American people. This is the mission of The New Center, which aims to establish the ideas and the community to create a powerful political center in today's America.

THE NEW CENTER

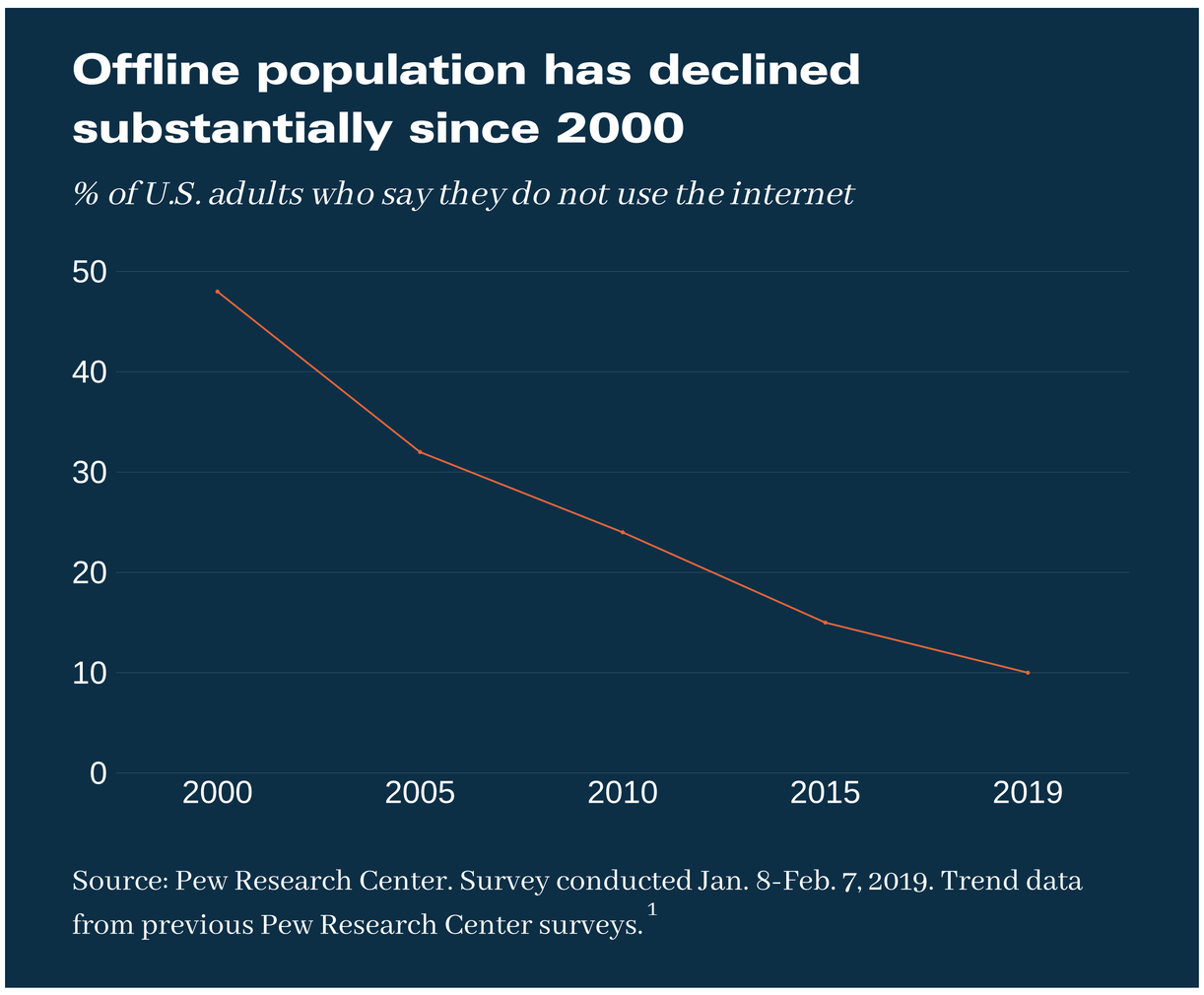
1808 I Street NW, Fl. 5
Washington, D.C. 20006
www.newcenter.org

Executive Summary

As America's internet dependence has skyrocketed, so have the malignant, often state-sponsored cyber attacks that steal American trade secrets, hold city networks for ransom, and spy on federal online activity.

Federal agencies, states, and critical infrastructure companies rely more and more on internet-connected systems, and their lack of cyber preparedness poses increasingly serious threats to our economic and national security.

In this paper, The New Center will explore several actions that federal leaders and policymakers can take to improve our national cybersecurity.



In summary, America must:

- **Support public education for cyber hygiene.** Americans from a young age should have access to classes that teach about the internet, networks, computers, and computer hygiene.
- **Pass the Internet of Things Cybersecurity Training for Federal Employees Act.**[2] This would require the Office of Management and Budget (OMB) to ensure that federal employees understand the vulnerabilities of Internet of Things (IoT) devices like smart watches, home appliances, and cars.
- **Expand the Continuous Diagnostics and Mitigation (CDM) model to critical infrastructure and to the states.** The CDM program, which scores cybersecurity levels among federal agencies in order to compare them, would be an excellent model for U.S. states and critical infrastructure entities. With more funding, the Cybersecurity and Infrastructure Security Agency (CISA) could allow states and critical infrastructure businesses to opt into a parallel program in which CISA provides reviews and recommendations for their cybersecurity.
- **Establish a standard protocol for how (and when) to get rid of legacy software.** Federal agencies should be prepared for how to get rid of their software before it goes out-of-date.
- **Create hierarchical requirements for two-factor authentication.** All workers accessing sensitive federal systems should be required to use two-factor authentication (2FA). Users with the most privileged access controls should be required to use 2FA with a physical key.
- **Define America's role in cyber law internationally.** The U.S. should take a more active role in setting cybersecurity standards in the international space. If America doesn't do it, another nation will.

Stuxnet, the Worm heard round the World

IN 2010, IRANIAN NUCLEAR TECHNICIANS AT THE NATANZ URANIUM ENRICHMENT PLANT HAD A PROBLEM.

As they worked to advance Iran's illicit uranium enrichment program, they were hitting a spate of bizarre equipment failures. Their plant's centrifuges—tubes that spin at supersonic speed to separate isotopes in uranium gas—were spinning out of control, and no matter how many times they were replaced, the new ones behaved the same. Even the inspectors from the International Atomic Energy Agency were perplexed.[3]

This was the advent of Stuxnet, a virus so potently sophisticated that it confounded the world and redefined the possibilities of cyber warfare. Although it infected thousands of unwitting computers to arrive at its final destination, the virus was only primed to activate within a highly specific array of Siemens centrifuges used in the Iranian nuclear program. It was a virus so controlled that it was self-destructing; it had an expiration date of June 24th, 2012, and would check the computer's internal clock to decide whether to proceed or shut down. It had an unprecedented total of four zero-days, or previously undiscovered operating system vulnerabilities that are typically cracked very scarcely. And it intercepted internal status reports with a loop of fake commands to make the infected computer seem fine. Never before had such a masterful virus hit the international spotlight.[4]

WHAT WERE IRAN-U.S. RELATIONS AT THE TIME?

In a word, tense. In February 2009, Iran announced its first successful satellite launch on the anniversary of the Islamic Revolution. In September, President Obama and other leaders accused Iran of building a secret nuclear plant, which it quickly confirmed.[5] Despite these challenges, President Obama continued to participate in international talks on ways to limit Iran's nuclear capabilities, culminating in the Joint Comprehensive Plan of Action (also known as "the Iran deal") in 2015.

Stuxnet, the Worm heard round the World

Two years later, White House officials confirmed expert suspicions: Stuxnet was indeed a calculated, immaculately designed cyber attack co-authored by the U.S. and Israel. Intent on slowing Iran's progress on building an atomic bomb, President Obama had covertly ordered the launch of Operation Olympic Games, a project from the Bush administration, to develop malware to disrupt Iranian attempts to build a nuclear weapon.

The operation was a challenge; Iran had strategically air-gapped the Natanz plant's computers from the internet, forcing the operation to seek roundabout access. Unable to tap into the computers remotely, the operation instead used USB flash drives to infect computers from five external firms with ties to the targets. The virus then passed from machine to machine until it reached its final destinations. Over the course of its run, it destroyed 1,000 out of 6,000 Iranian centrifuges and infected more than 100,000 computers worldwide. [6]

Most notable of all, however, was Stuxnet's vast implications. The computer worm shocked nations around the globe for being the first-ever cyber attack to crash through the digital-physical divide and destroy something in the real world. And as nations slowly discovered, Stuxnet would just be the beginning. Today, Stuxnet is the first of three known malware strains to attempt to damage physical equipment. The second was Industroyer, the malware used by Russia to trigger blackouts in the city of Kyiv, Ukraine between 2015 and 2017 but failed to cause the lasting damage it intended. [8] The third was Triton, a rare malware that aimed to destroy industrial control equipment in a Saudi Arabian oil refinery in 2017. [9]

WHAT IS AIR-GAPPING?

Air-gapping is a security measure in which the owner of a network separates it from the internet to shield it from cyber attacks. This kind of protection is common for high-risk systems that require high security, such as classified military networks, industrial control systems (ICS) that command critical infrastructure (CI), and online payment systems. At the Natanz plant, Iranian leaders air-gapped the machines controlling their nuclear equipment, plus all the computers these machines were connected to. While air-gapping is theoretically very secure, some companies only "air-gap" their systems with software firewalls, whose security holes can let hackers slip through. But even the truest form of air-gapping isn't perfect; like the world saw at the Natanz plant, infected USB drives can also do the trick.[7]

Implications for U.S. National Security

Stuxnet, Industroyer, and Triton together wrote the introduction for a new chapter in the story of cyber capability. As the digital arms race heats up at record speed, cyberspace has become a new battleground threatening the national security of countries around the world. And despite the sophistication of America's Stuxnet offensive, our cyberdefense needs work.

In 2015, an employee at the U.S. Office of Personnel Management (OPM) discovered that over the course of a year, hackers had stolen the highly sensitive personal information of 22 million current and former federal employees and their spouses. (For context, approximately two million people are currently on the federal payroll.[10]) The FBI later arrested a Chinese national for his role in the attack.[11] In 2017, just days before President Trump's inauguration, a Romanian couple targeting a trove of random email addresses managed to (accidentally) wrest control of White House cameras.[12] And in 2018, the Chinese government hacked the computers of a Navy contractor to steal 614 gigabytes of highly sensitive data on undersea warfare, including clandestine plans to build supersonic missiles for American submarines.[13] If the success of these attacks is any indication of the state of cybersecurity among federal agencies, the U.S. has a problem—and the U.S. Government Accountability Office (GAO) has no qualms pointing it out.

In fiscal year 2017, America's federal executive branch civilian agencies reported over 35,000 information security incidents according to GAO. But while GAO has made over 3,000 recommendations to federal agencies to address cybersecurity vulnerabilities, about 700 still have yet to be implemented.[14]

The OPM Hack: Government's Wake-up Call

The hackers, widely assumed to be Chinese actors operating on behalf of the state, filched information from approximately 21.5 million current and former government applicants and their spouses.[15] The information stolen were these applicants' SF-86 forms, or the 127-page questionnaires on everything from applicants' personal finances to their past drug abuses to their psychiatric care, all used to clear government workers for highly sensitive and secret jobs.[16] The implications for national security were significant; for everyone who has ever worked for the federal government pre-2015, China knows their secrets.

According to a report by Symantec, the security firm that uncovered Stuxnet, the U.S. faced the greatest number of targeted attacks of any country between 2016 and 2019. In 2018, American authorities made an unprecedented total of 49 indictments against targeted attackers from America's top cyber adversaries, up from four in 2017 and five in 2016.[17]

Implications for the U.S. Economy

Cybersecurity failures don't just affect Americans' safety; they affect our wallets, too. American states, cities, and federal agencies have lost billions to ransoms, and to the recovery and incident mitigation costs that follow them. In June of 2019, for example, Riviera Beach and Lake City, Florida parted with a combined $1 million to pay off hackers. The White House estimates that cybersecurity attacks cost the U.S. economy between $57 billion and $109 billion in 2016 alone. For context, the Center for Strategic and International Studies (CSIS) estimated that cybercrime costs the global economy $600 billion a year, or one percent of global GDP. [20]

But cybertheft goes deeper than hackers swiping information from American government and firms in exchange for bribes. It extends to an invisible economic tug-of-war between the U.S. and China, in which China steals billions of dollars worth of intellectual property (IP) from American firms that struggle to protect their computers. According to the Justice Department, more than 80% of economic espionage cases brought to it from 2012 to 2019 have implicated China, and a CNBC survey found that one out of five North America-based companies say China stole their IP last year. [21]

As the U.S. continues to lose this game, the costs are racking up. The United States Trade Representative, which conducted a seven-month investigation of the problem, reported that Chinese state-sponsored IP theft currently costs the U.S. between $225 billion and $600 billion every year. Dmitri Alperovitch, a Russian-American computer security industry executive, has dubbed it a "historically unprecedented transfer of wealth." [22]

Some experts warn that over time, this massive transfer could eventually hollow out the U.S. economy. As the political scientist P. W. Singer and Director of Cybersecurity Initiatives Allan Friedman write in Cybersecurity and Cyberwar, "[While] each loss from cyber espionage is too small to be fatal on its own... their accumulation might prove crippling." [23]

What about Talk of a Cyber Catastrophe?

Copious cyber attacks on American government combined with a lack of U.S. preparedness have together stoked fears of an impending cyberpocalypse. While our cybersecurity is indeed vulnerable, warnings of a cyberpocalyptic accident seem overblown.

Sophisticated cybersecurity attacks like Stuxnet require extensive expertise, personnel, and capital, and most nations would struggle to muster the resources to pull one off. Besides, cyber weapons have yet to be physically harmful to people. As R Street Institute cybersecurity fellow Paul Rosenzweig put it, "More people have died from squirrels the past year than cybersecurity problems." [25]

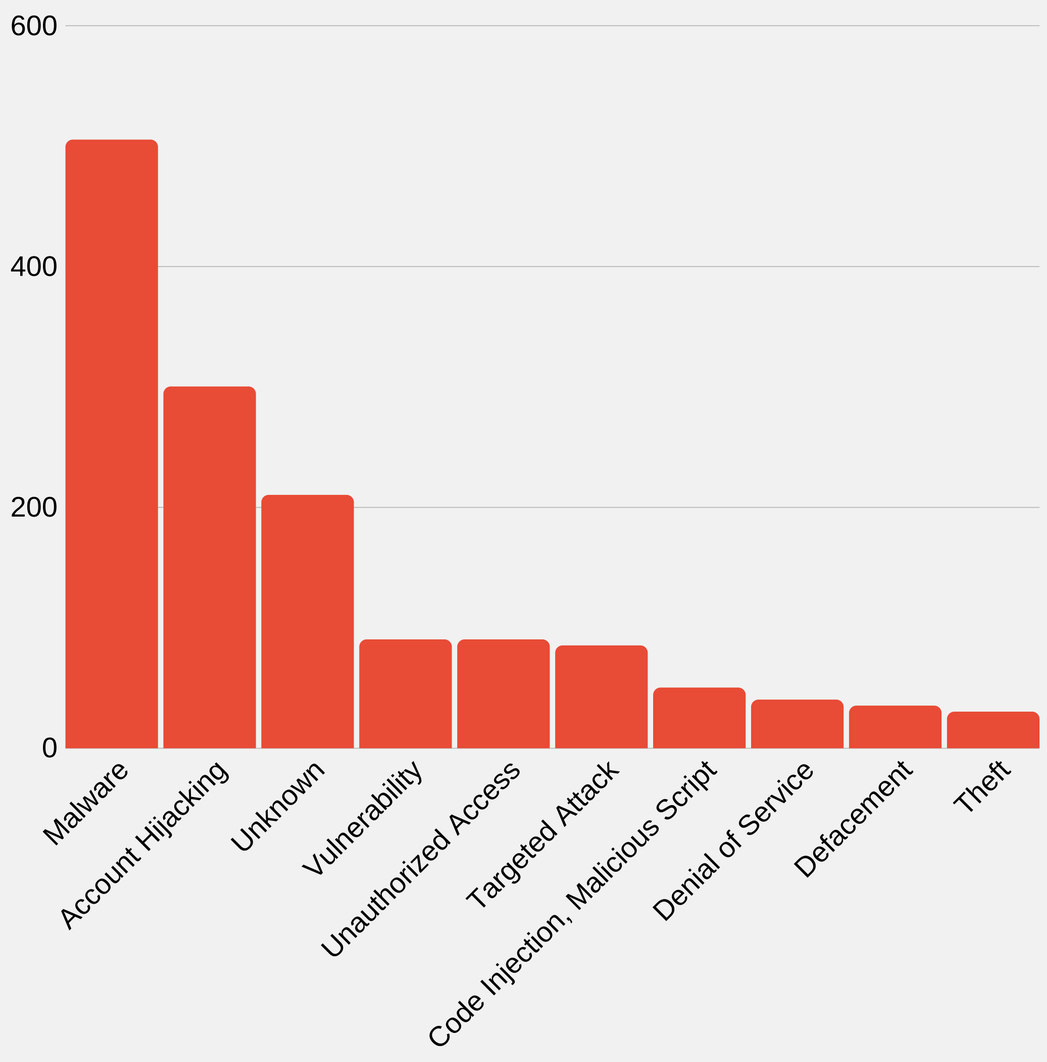
What Is a Cyber Attack?

Cyber attacks tend to come from malware, malicious software that falls into a few distinct categories: ransomware, viruses, worms, and bots.

Ransomware is a type of malware that encrypts a target's files, with the hacker typically demanding money in return for the de-encryption code. (Many American cities know this form of attack increasingly well.) Viruses and worms spread copies of themselves from computer to computer often through social engineering tricks that manipulate users, like deceptive emails with infected attachments. Once inside a computer, viruses and worms can modify and delete files, log keystrokes, create secret backdoors, and generally commandeer entire systems.

TOP 10 ATTACK VENDORS IN 2018-2019

(Number of reported breaches)



According to the computer security firm McAfee, malware was the most common type of cyber attack between 2018 and 2019. Malware is often random, with hackers dredging up targets much like trawling boats pull nets through the ocean, seeing what sea creatures they can catch. Less common were targeted attacks, where hackers actively pursue specific targets.

Source: McAfee Labs, 2019. [28]

While the terms "virus" and "worm" are interchangeable in terms of their effects, there's one key difference. Viruses attach themselves to a certain host file, requiring this file to run before they can run their own code, while worms exist independently. Stuxnet, for example, was technically a worm—not a virus. [26]

Bots, often the products of successful viruses and worms, are computers that have been secretly hacked—with their owners none the wiser. Hackers can covertly take over millions of vulnerable computers to exploit their collective resources, forming massive zombie armies or botnets they can deploy at will.

Among other things, hackers can manipulate these expansive botnet armies into launching Distributed Denial of Service (DDoS) attacks on larger, more powerful targets like corporations and governments. In this type of attack, such a large number of computers request to visit a website that it becomes overwhelmed and shutters temporarily.

In 2011, for example, the Syrian regime lent its supporters botnet tools to launch DDoS attacks on anti-government websites. And in 2008, a worm called Conficker exploited a Microsoft Windows vulnerability to form a botnet out of the 7 million users who didn't install a security patch. [27]

The Problems

Computer Hygiene in the American Workforce

In 2008, an American soldier picked up a mysterious flash drive in the parking lot outside a U.S. military base and plugged it into a network at the U.S. Central Command, one of the eleven combatant commands of the Department of Defense. The flash drive uploaded a worm designed by foreign intelligence to scan the base's computers for data, implant secret backdoors, and link to command-and-control servers. (These servers are computers that rule infected systems.)

The Pentagon spent 14 months cleaning it up.[29]

In cyber terms, the incident was a "candy drop": when a hostile actor leaves a USB drive lying around as bait for curious targets to plug in—unwittingly jamming the enemy straight into the target system's information jugular, bypassing access controls. Like many cyber schemes, these attacks prey on the lack of basic IT training among not just government employees, but the public alike.

People in the physical world are the first line of defense against cyber threats in the digital one, so it's a problem when they receive little to no training identifying common scams. This problem is ongoing, and if unaddressed, will only continue to pose critical threats to our systems. If an incident back in 2008 seems too far removed, consider that when hackers seized control of White House cameras days before President Trump's 2017 inauguration ceremony, it was because a White House employee opened an infected attachment from an email phishing scam.

While government agencies are working toward solving this problem, they focus narrowly on the training of federal and cybersecurity professionals. The Cybersecurity and Infrastructure Security Agency (CISA), a cybersecurity-focused agency established in November 2018 within the Department of Homeland Security (DHS), has developed free cybersecurity training and exercises for government agencies.[30] The National Security Agency has developed a free online course on cybersecurity, and CISA has a National Cybersecurity Awareness Program. [31]

At the Department of Commerce, the National Institute of Standards and Technology (NIST) has pioneered the National Initiative for Cybersecurity Education, which partners with government, academia, and the private sector to develop cybersecurity education, training, and workforce development. [32]

Although these initiatives are important, they are not commensurate with the scale of America's cybersecurity challenge. Fundamentally, very few Americans understand even the basics surrounding the internet, let alone how to protect themselves or their devices.

In Pew Research's 2014 Web IQ test that surveyed a nationally representative sample of 1,066 internet users, only 23% of respondents correctly answered the question, "Are the internet and the world wide web the same?" (The answer: they are not.) [33]

The problem transcends generations. In 2016, the Stanford History Education Group found that surveyed students at every education level could not distinguish between credible and non-credible information online, with less than 20% of surveyed high school students able to peg a highly doctored photo for what it was.[34] And in 2018, when the Federal Trade Commission tallied up fraud reports from people who provided their ages, it found that Americans in their 20s were nearly three times as likely to have lost money to fraud than those in their 70s.[35]

It's critical for internet and cyber hygiene training to be available to everyone. Like how herd immunity can protect an entire community from disease, only universal training can protect an entire system—because it only takes one to compromise it.

Basic education surrounding networks, cyber attacks, and computer hygiene should come early, be ongoing, and be available to everyone. The same way that public schools are required to offer courses in health, a lifelong pursuit that applies to all, they should also offer courses on these topics. The internet has become completely inseparable from every facet of our personal and professional lives—and will only soar in importance in the coming years. As a nation, shouldn't we all understand how it works, and by proxy, how to protect the systems we depend on?

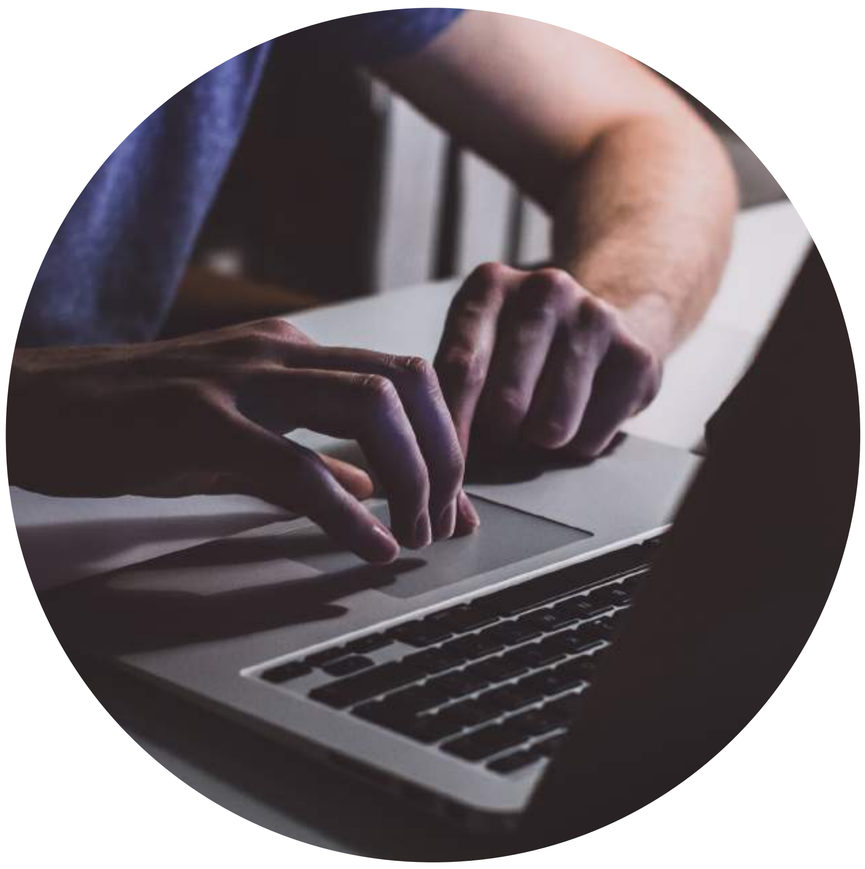
"The problem is that individual bad security decisions make many others worse off. When you fail to update your personal computer's defenses, its compromised security could add it to a botnet that is attacking the wider internet. When a company fails to come clean about an attack, it allows... the vulnerabilities they targeted to be exploited elsewhere."

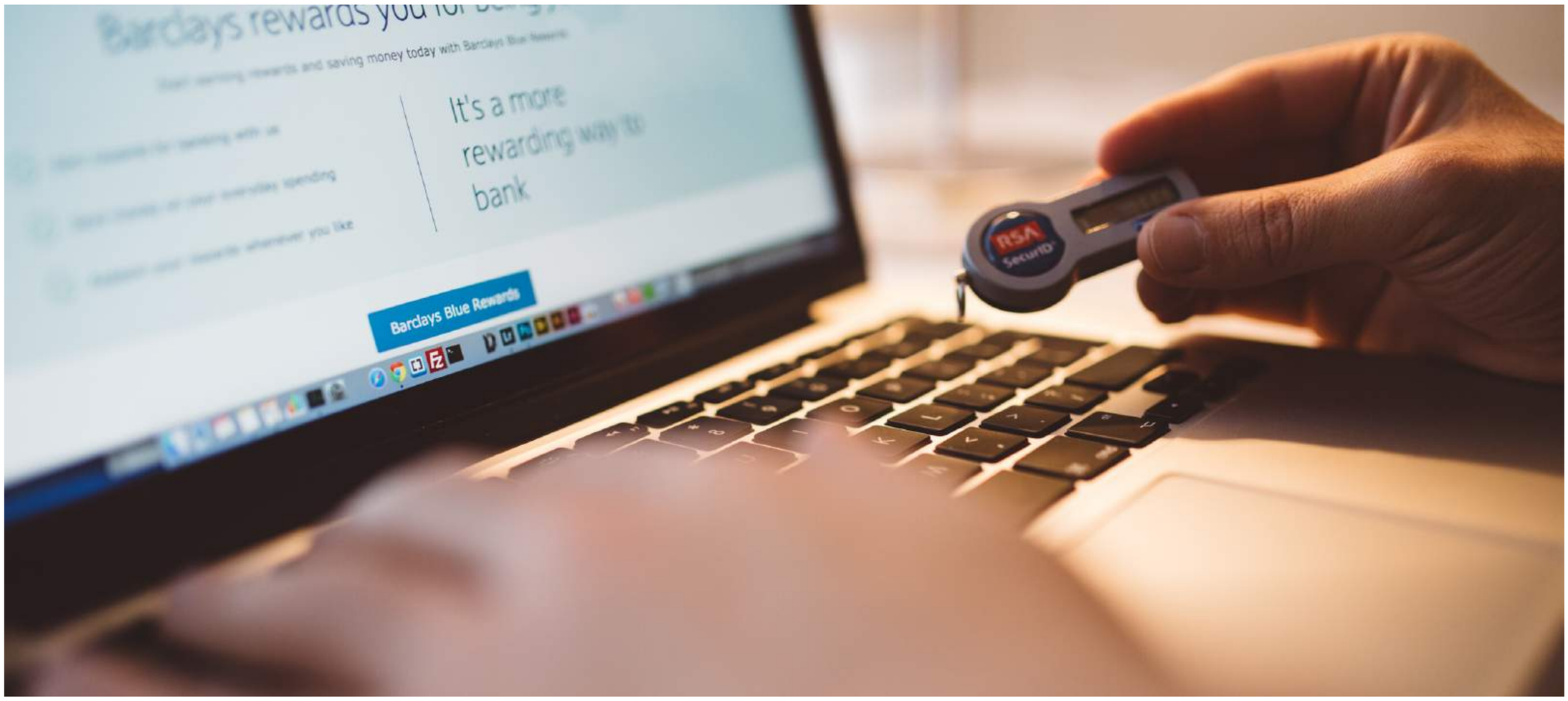
—Cybersecurity and Cyberwar

Do you know your router password?

In 2017, Reichelt Elektronik, an electronics retailer, commissioned a poll of British adults on their use of routers, the technology that connects people's devices to the internet by "routing" the traffic.[36] Router control is password-protected, but when internet service providers (ISPs) install routers in people's homes, they tend to use identical default passwords.

In order to protect their network, then, a customer needs to change the default password to a unique one—but according to Reichelt Elektronik's poll, 55% of surveyed adults never changed their passwords from the originals.[37] This means that huge swathes of people across the U.K., the U.S., and other countries could be using routers with the exact same passwords as other clients of their respective ISPs, making tons of connections easy prey for hackers. This is just one of many examples of how the power of our everyday tech has rapidly outpaced our understanding of it—a development that threatens our security.





Measuring Cybersecurity

Before May 2019, measuring cybersecurity among federal agencies was a confusing patchwork of different agencies using different strategies at different times—which meant measuring any agency's state of cybersecurity up against another's was close to impossible. What, after all, is a "good" level of security when there's nothing to compare it to?

While some agencies did volunteer to share information with the Continuous Diagnostics and Monitoring (CDM) program, a program by CISA to provide tools for tracking suspicious traffic on their networks, many agencies did not, posing a challenge to federal cohesion.

In 2019, this changed radically when the White House Office of Management and Budget (OMB) forced all federal agencies to share information with the CISA's CDM. [38] And in May 2019, about a year after CISA was formed, the DHS granted a $276 million contract to ECS Federal, an IT company, to create a federal dashboard to conveniently display the results of all federal agencies, side-by-side, to CISA. [39] In 2020, this display will include CDM's newest and perhaps most groundbreaking tool for measuring cybersecurity: AWARE, or the Agency-Wide Adaptive Risk Enumeration, which will score each agency's cybersecurity risks. By checking how agencies are performing on basic security measures like vulnerability, patch management, and configuration management, the AWARE algorithm will "track millions of assets across the entire federal security landscape." [40]

Empowered with this critical information, CISA will be able to compare federal agencies' cyber scores to the federal average over time, with federal leadership deciding who else will see the numbers.[41]

Legacy Software (and Habits, Too)

Most Americas own smartphones.[42] But when they visit their settings, how often do they discover software update alerts? At any given moment, odds are that many Americans have yet to install a software patch that fixes a vulnerability. And the longer Americans wait, the more susceptible their devices are to hackers in the digital arms race.

The government has similar problems, where delays on software patches, the use of legacy software, and outdated tech habits pose massive threats to federal networks. When Microsoft officially ended support for its 13-year-old operating system Windows XP, for example, an estimated three percent of the Pentagon's computers were still running on it. (So do Russian President Vladimir Putin's computers, curiously enough.[43]) And despite the Navy's project to switch off of the OS, challenges with the upgrade compelled the Pentagon to simply give contracts to Microsoft for extended support.[44]

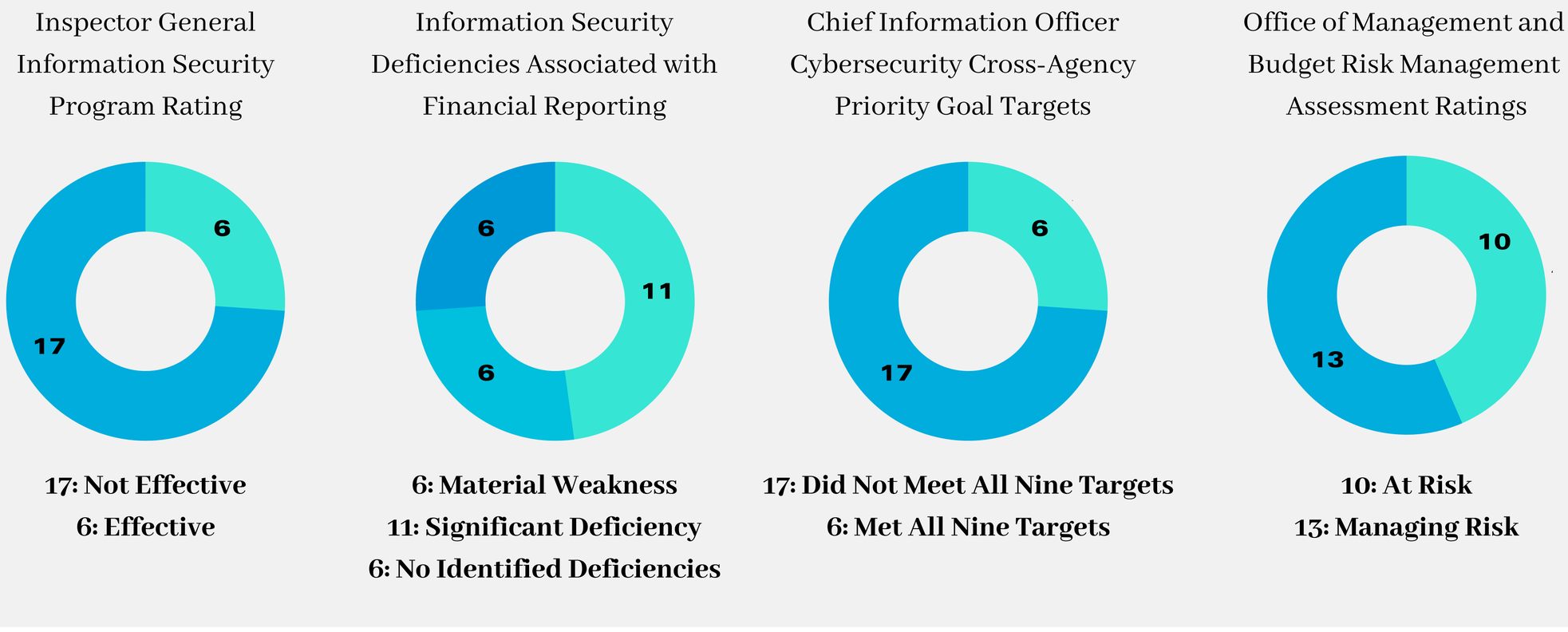
Other legacy habits include not requiring multi-factor authentication for government employees to access government networks. Multi-factor identification is a log-in process that involves more than just a password; a user must provide at least one other form of identification to prove they are who they say. This can involve receiving a security code via text, phone call, or app on one's phone, or using a physical "key" to plug into one's computer. In other words, a user must have both something they know (their password) and something they have (their phone or physical key).[45] The gold standard of basic security practices, multi-factor authentication is critical to protecting databases and networks from easy intrusion. Stanford University, which requires two-factor authentication (2FA) for students logging into its systems, says of the concept:

> **"In today's cyber threat landscape, static login credentials alone are no longer sufficient to protect our systems and data. These credentials are highly susceptible to phishing and offline cracking (if the corresponding password hashes are exposed). Two-step authentication adds a dynamic component to logins, which significantly mitigates this risk."**[46]

While the government took steps in the right direction in 2018 by requiring 2FA for the administrators of federal agency dot.gov domains and registrar accounts, unlike OPM, it still doesn't require the practice for all of its system's users. In early 2018, OPM distinguished itself by rolling out a requirement for two-factor authentication for all users of its usajobs.gov site, likely a result of its hemorrhage of sensitive personal data to Chinese hackers in 2015.[47]

Legacy Software (and Habits, Too)

Fiscal Year 2017 Indicators of the 23 Selected Civilian Agencies' Effectiveness in Implementing the Federal Approach and Strategy for Securing Information Systems



Source: GAO analysis of agency fiscal year 2017 *Federal Information Society Modernization Act of 2014* and agency financial reports for fiscal year 2017. [48]

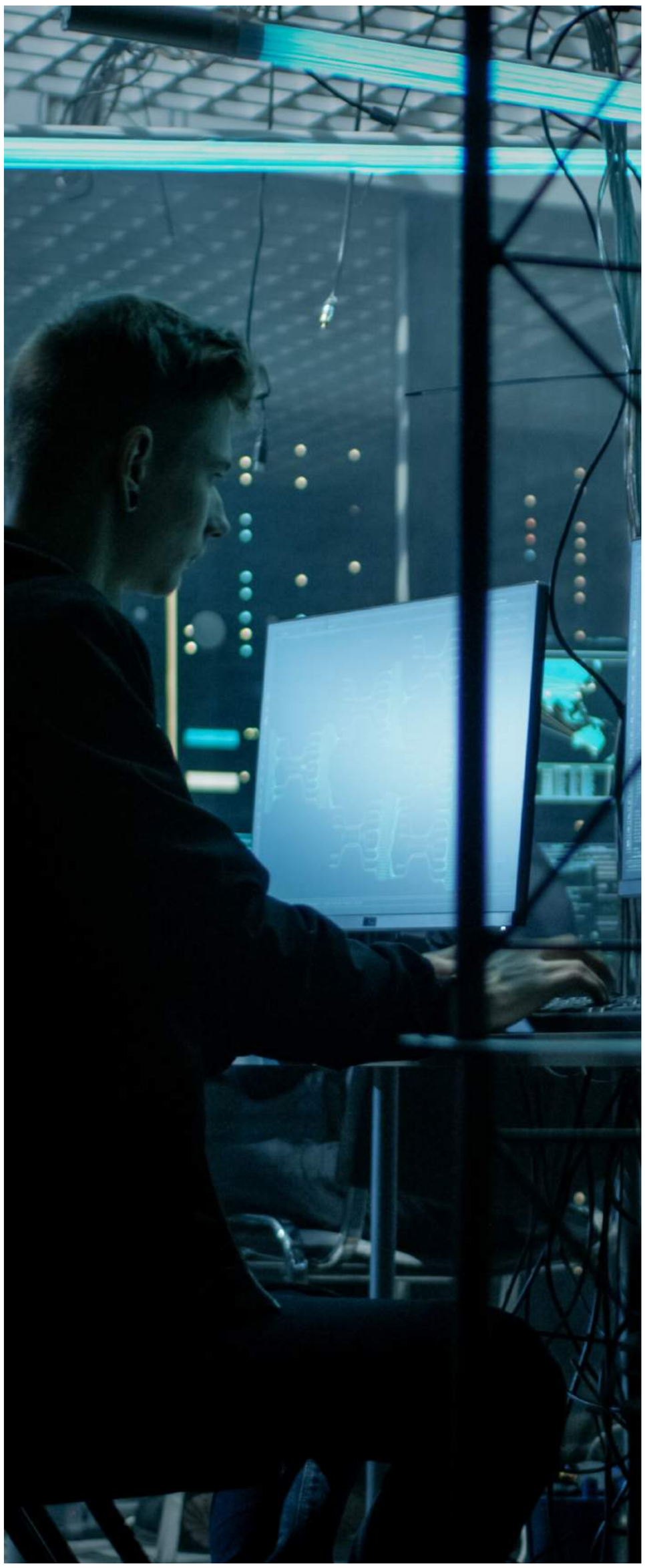
But even blanket requirements for 2FA are no silver bullet; as Russell Brandom writes in Wired, "If you can break through anything next to that two-factor login—whether it's the account-recovery process, trusted devices, or the underlying carrier account—then you're home free." Breaching a wireless carrier like AT&T or Verizon, for example, would easily permit a serious hacking group to pilfer someone's security code from a text. But this danger isn't hypothetical.

The security firm Cybereason reported in February that a cyberthief had recently attacked 500,000 targets using ransomware that helped them steal users' 2FA tokens. [49] NIST, which caught onto this glaring security gap relatively early, withdrew its support for SMS-based 2FA in 2017—but per the 2018 government-wide rule, administrators of registrar accounts can still use this method. [50]

The government needs to develop a clear, standardized protocol for when and how to update and replace its agencies' aging operating systems.

And as for multi-factor identification, the government should work toward requiring 2FA not just for administrators, but for all federal workers who use sensitive federal networks. This 2FA should be hierarchical, with prescriptions for different types of 2FA based on degrees of access; administrators should use a 2FA that doesn't involve SMS and is therefore tougher to crack, while users with fewer access privileges could still use cell-based access codes.

The Cyberskilled Need Apply



Government cybersecurity will only be as effective as the professionals who develop it, which is a problem when there aren't enough of them.

According to a report from the Center for Strategic and International Studies (CSIS) called A Human Capital Crisis in Cybersecurity, the U.S. government had only 3 to 10% of the cybersecurity professionals it needed in 2010—a problem that persists today. [51] According to a heat map of cyber job postings by CyberSeek, the public sector only employed about 65,000 professionals between October 2018 and September 2019 but needed 33,000 more—a 33% deficit. [52] And as the demand for cybersecurity workers has surged in both the public and private sectors, the hiring frenzy has squeezed existing labor pools, leaving the government at a stark disadvantage.

Responding to this critical shortage, the government is currently experimenting with many ways to redress it. The Cybersecurity Talent Initiative, an 11-agency public-private partnership, recruits recent college graduates in exchange for the promise of a job in the private sector after a two-year government stint. [53] The Federal Cyber Reskilling Academy trains non-cyber federal employees in cyber skills. [54] Government agencies like the DoD host contests to identify cyber talent. And perhaps most importantly of all, the DHS is shifting away from the traditional "post-and-pray" method of government hiring, whereby the government quietly posts vacancies online and hopes that qualified professionals will surface. Now, DHS sends recruiters to proactively poach cyber talent, and has even launched a Cyber Talent Management System to offer market-based pay to tech professionals. [55]

More funding for hiring cyber talent—and paying them well—will be critical to pulling federal cybersecurity up to a new bar.

But there are other ways the government can kindle its techie talent pools. One strategy could be promoting pockets of culture that are friendlier to Silicon Valley expats, like the culture of the United States Digital Service (USDS). Founded by President Barack Obama and housed within the Executive Office of the President, the USDS is a self-described "start-up within the government" that attracts computer science talent mission-critical to helping a variety of federal agencies tackle their tech problems. With a culture more akin to start-ups than government, the USDS features photos on its flagship site of employees donning hoodies and tees, a stark contrast to traditional suit-and-tie government jobs. [56] The USDS has also striven to adopt practices that attract private sector talent in other ways, like slashing its hiring time. [57]

More Public-Private Partnerships, Especially in Critical Infrastructure

In February of 2015, months before OPM discovered its notorious breach, the security firm ThreatConnect published a report about a suspicious domain. The domain was named opm-learning.org and registered to Iron Man's alter ego "Tony Stark," implicating a powerful Chinese hacking group known for registering domains to Marvel characters. In April, when an OPM security engineer discovered malware in its own systems, he found that it linked to the domain name opmsecurity.org that was registered to "Steve Rogers." Per Marvel lore, Steve Rogers is Captain America's predecessor, transforming into the superhero after quaffing a serum.[58]

If OPM had learned of malware linked to a domain named opm-learning.org, it might have scoured its own systems and discovered its debilitating hack sooner—but the lack of cyber collaboration between the public and private sectors preempted this.

As it stands, there's little cybersecurity sharing between America's public and private sectors, despite the fact that both are fighting the same digital adversaries. This cyber collaboration deficit poses problems when American industry works so closely on public projects. Although OPM reports that only 2.1 million civilian workers were serving the federal government in 2019, this figure conceals the millions of private contractors who don't work for the government directly but still work on public projects.[59] In 2019, for example, the federal government employed more than 4.1 million contractors from over 10,000 different companies.[60] This creates billions of digital links between private and public networks, systems, and databases. As a result, a cyber blow to the government can hurt industry, and a cyber blow to industry can hurt government.

This lack of cyber cooperation poses an especially concerning problem for critical infrastructure, or CI such as water, electricity, oil, gas, and chemical production facilities. According to CISA, there are 16 critical infrastructure (CI) sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[61] While these industries do receive topline regulation from federal bodies, they are, for the most part, privately controlled. NIST works with these industries' regulatory bodies to help guide cybersecurity best practices, but it's the regulatory bodies, not NIST, that control protocol and implementation.[62]

CISA'S 16 CRITICAL INFRASTRUCTURE SECTORS

Chemical, Communications, Dams, Emergency Services, Financial Services, Government Facilities, Information Technology, Transportation Systems, Commercial Facilities, Critical Manufacturing, Defense Industrial Base, Energy, Food and Agriculture, Health Care and Public Health, Nuclear Reactors and Materials and Waste, and Water and Wastewater Systems.[63]

More Public-Private Partnerships, Especially in Critical Infrastructure

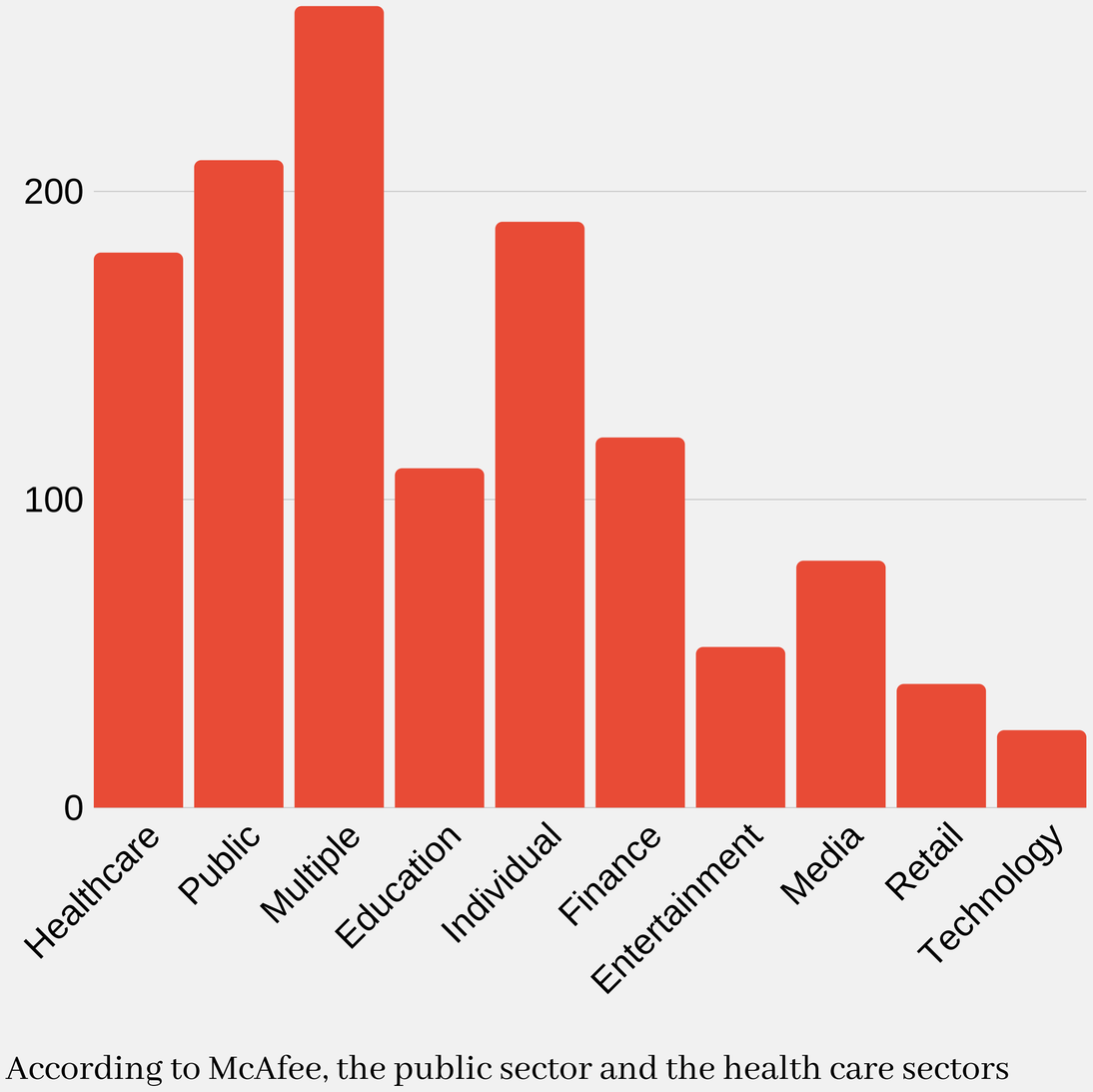
The Director of CISA, Christopher Krebs, has suggested that this lack of government involvement could pose dire threats to American CI, which is failing to keep up with basic cybersafety standards. In his 2019 article in Lawfare, Krebs describes a few concerning examples.

"CISA is currently aware of a system that controls water pumps, one controlling an oil and natural gas facility, and one controlling emergency management equipment that can be accessed without a password and modified by anyone with an internet connection. Unless Congress acts, systems that support critical functions that everyday Americans rely upon could remain wide open to attack, but there's little we can do to protect them." [65]

Director Krebs goes on to explain that CISA has no way of knowing who, exactly, owns and operates many of these vulnerable systems, which are only linked to internet protocol (IP) addresses. Only the owners' ISPs know their customers' names, but it's illegal for ISPs to divulge this information to CISA. As a result, CISA can't swoop in with cybersecurity first-aid—even in the event of a massive breach.

To change this, Senators Ron Johnson (R-WI) and Maggie Hassan (D-NH) introduced a 2019 bill that would grant CISA the power of the administrative subpoena. With it, CISA would be able to acquire the contact information of vulnerable entities from their own ISPs.[67] But the bill stirred up concerns about the privacy of the operators of critical infrastructure, plus questions surrounding how deeply intertwined the federal government should be in cyber problems that are legally private.

Top 10 Targeted Sectors in 2018-2019 (Number of reported breaches)



According to McAfee, the public sector and the health care sectors reported the highest number of breaches between 2019 and 2019.[64]

What Is an IP Address?

An internet protocol address is a unique number made of digits and periods assigned to every device when it connects to the internet. The Internet Corporation for Assigned Names and Numbers, or the internet-regulating nonprofit known as ICANN, helps to assign them. The numbers allow computers, servers, phones, cameras, sensors, and printers to identify and communicate with each other.[66]

On one end of the spectrum, the authors of Cybersecurity and Cyberwar suggest that the lack of forced cyber regulation could be a catastrophe waiting to happen. According to Singer and Friedman, our current absence of government-mandated cyber regulation is akin to the lack of shipping regulation before the Titanic sunk, or to the lack of nuclear power regulation before Three Mile Island, America's most severe nuclear accident.[68] On the other end, industry advocates like Paul Rosenzweig defend businesses as far swifter and more capable than governments, whose slow-moving regulations would theoretically tie them down. According to Rosenzweig,

> **"A friend of mine in the industry once told me, 'The attackers are a year ahead of the defenders, the defenders are two years ahead of the legislators, and the legislators are two years ahead of the regulators.' That's just the way it works. Our government is a slow-moving, hierarchical system. The cyber domain is a distributed, fast-moving system. Another friend of mine once said, 'The government is a Ford Edsel, and cybersecurity is a Tesla.' And I actually think that understates the difference."[69]**

Not all government efforts have been so controversial. Government has responded to the CI cybersecurity crisis in other ways, like by awarding nearly $30 million in private sector grants to fund innovations that protect power grids and oil pipelines. The Department of Energy is teaming up with industry to create recommendations for industrial control systems (ICS), which are increasingly targeted by cyber attacks.[70] As for efforts by CISA, the organization's own National Cybersecurity and Communications Integration Center (NCCIS) is partnering with industry to protect American cybersecurity, stop threats, protect against risks, and deliver products that underpin our critical infrastructure.[71] And CISA's National Infrastructure Coordinating Center (NICC) acts as an information-sharing hub between DHS and critical infrastructure entities when there are breaches.[72] One potential solution could be the expansion of CISA's CDM model to CI entities. CISA could launch a program just like CDM but for critical infrastructure, with CI businesses able to opt in or opt out of providing data in exchange for comprehensive cybersecurity reviews and recommendations from the experts. If CI companies opted in, it would expose private data to public eyes only voluntarily.

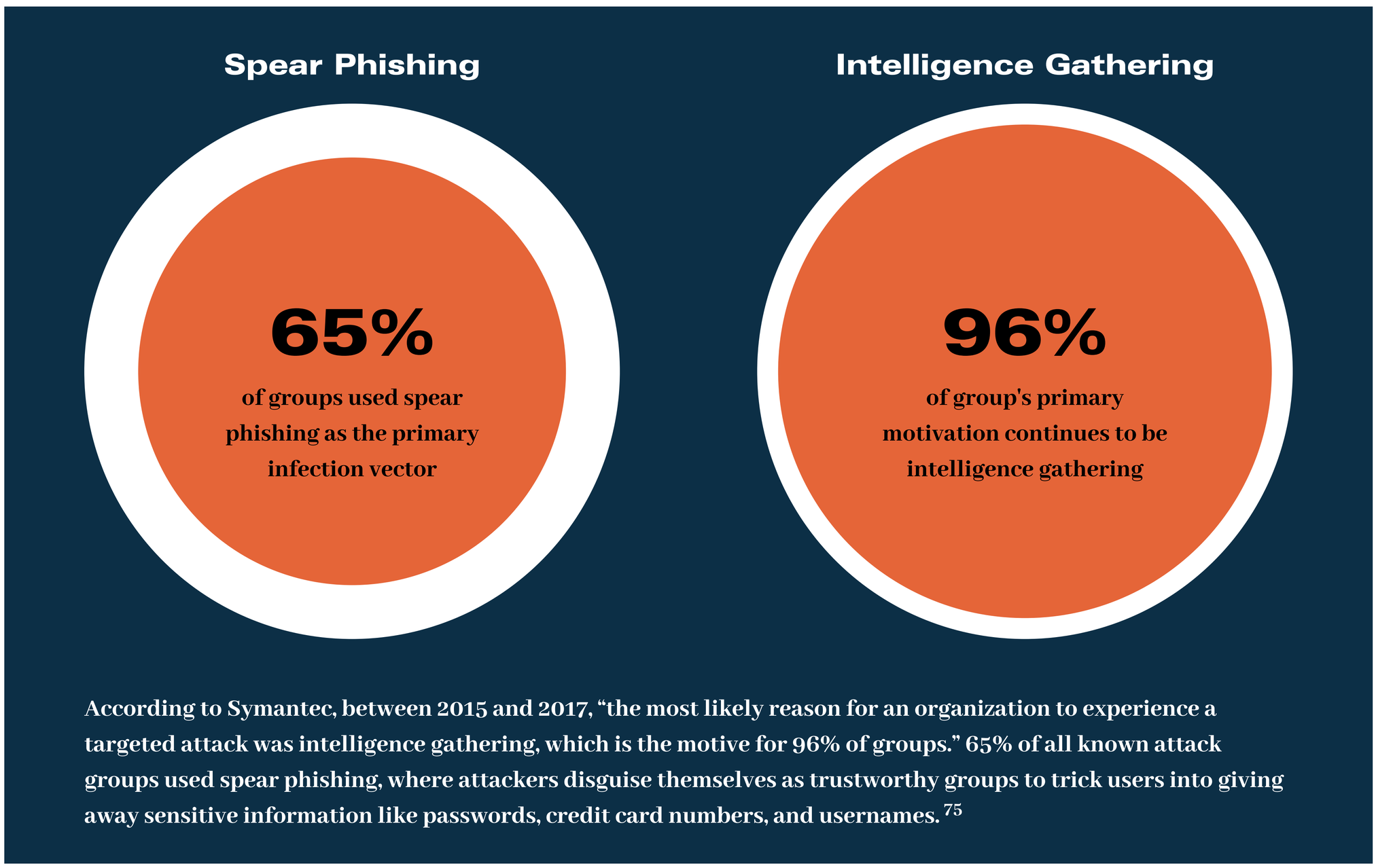
Going one step further, Congress could even fund a new CDM-style program administered by CISA for American states. With their facilities regularly held hostage by hackers, American states and major cities struggle just as much (if not more) to protect themselves. In the past two years, hackers demanding a ransom shut down Baltimore's computer systems on two separate occasions, and cities all around the country have witnessed massive surges in cyber attacks on their susceptible systems. Expert evaluations and recommendations from CISA could give states a sense of where to funnel their cybersecurity funding, and what, exactly, needs patching.

When it comes to the internet, all stakeholders are inextricably linked, and a security breach in one place has implications for security somewhere else. It's critical for the federal government to work together with industry and states alike to hash out a protocol for protecting the American people and the critical systems they depend on.

International Cyberspace and a Lack of U.S. Leadership

While the United States leads the world economically and politically, it's kept quiet so far on international cyber law. In 2018, when French President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace, a document declaring common best practices for cyber behavior internationally, the U.S. conspicuously failed to sign. [73] (So did China and Russia, the other major cyber powers.) The European Union has also outpaced the U.S. in other forms of digital law, like the General Data Protection Regulation. Abbreviated to GDPR, this groundbreaking privacy legislation debuted officially in 2018 and set rules for how companies could store users' personal data online. [74]

According to William Carter, the former Deputy Director and Fellow of the Technology Policy Program at the Center for Strategic and International Studies (CSIS), American reluctance to legislate probably stems from a hesitation to commit to norms it will certainly break. One of many provisions of the Paris Call, for example, encourages nations to "prevent... malicious cyber activities that threaten or cause significant... harm to individuals and critical infrastructure"—a tenet that, if followed, would have kept the U.S. from launching Stuxnet. The U.S. has no interest in agreeing to norms that constrain its own behavior only for Russia and China, its cyber adversaries, to take advantage.



International Cyberspace and a Lack of U.S. Leadership

But defining cyber norms doesn't have to mean restricting American power. The U.S. could develop norms with like-minded countries that reflect the way the U.S. currently operates. Then the U.S. could encourage other countries to sign onto formal mechanisms that govern and describe these behaviors, making it easier for countries new to cyberspace to comply.

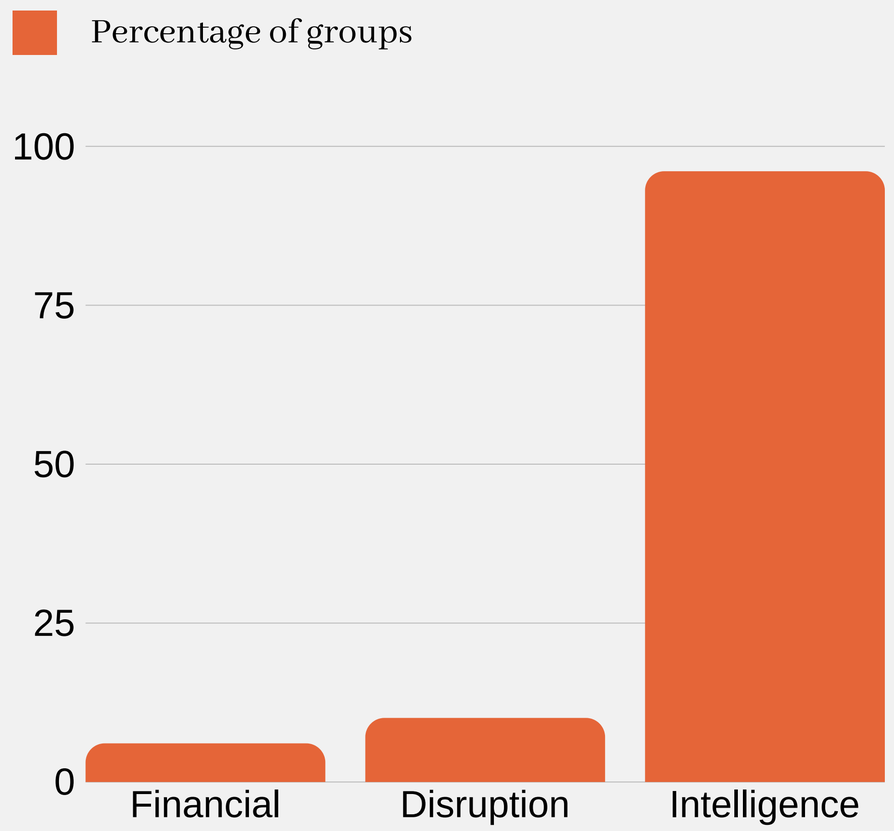
According to Carter in an interview with The New Center, a reluctance to commit to certain norms doesn't mean that the U.S. shouldn't play a role in setting other ones. Carter sees significant benefits to an American role in participating in agreements, even if the U.S. can't promise anything groundbreaking.

"At the end of the day," Carter opines, "we benefit from establishing a common understanding for how states should operate in cyberspace... If we can establish a common baseline of what we consider to be inappropriate behavior, hopefully it will prevent uncontrolled escalation dynamics, provide some degree of transparency, and help us to establish international coalitions to impose consequences on malicious actors who engage in bad behavior in cyberspace—all of that is to our benefit."

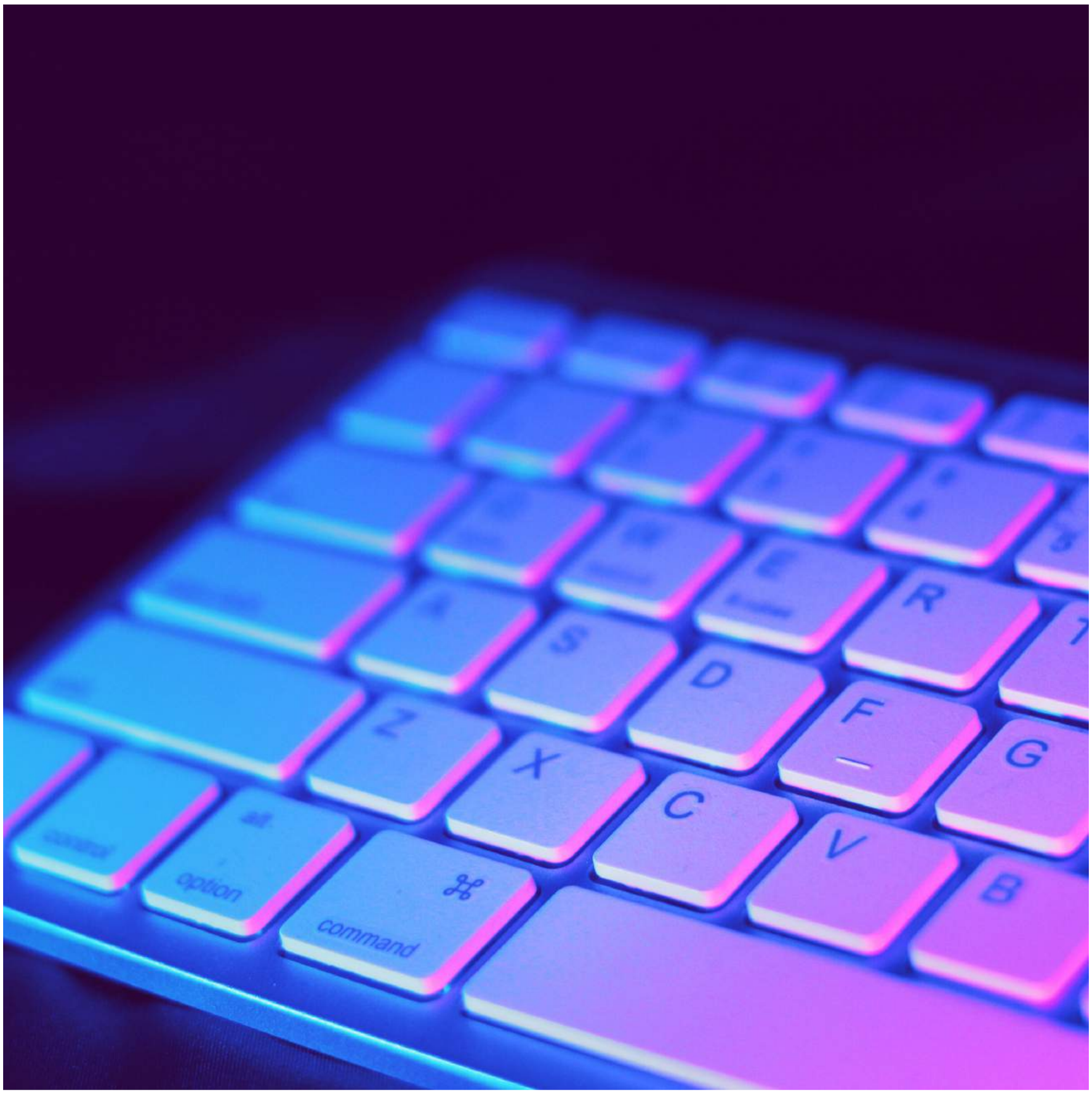
Like the laws of warfare, laws in cyberspace can also accommodate justified forms of aggression. "In war, you accept that your adversary is going to shoot at you," he explains, "but that doesn't mean that you don't try to shoot back. You can still have things like the Geneva Convention defining what is and is not appropriate behavior for nation states at war. That's the type of thinking we need to get to—it's a much more nuanced conversation."

The alternative, Carter says, is to let America's cyber adversaries—Russia and China—take the leadership role. It's a space the U.S. shouldn't cede.

Targeted Attack Group Motives (All Time)



Of all targeted attacks known to Symantec, intelligence-gathering has been their most common motive. [76]



The Solutions

The Solutions

Support public education for cyber hygiene.

It's time for us to step up as a nation. Americans from a young age should have access to classes that teach about the internet, networks, computers, and computer hygiene.

Pass the Internet of Things Cybersecurity Training for Federal Employees Act.[77]

Introduced in 2019, the act would require the Office of Management and Budget (OMB) to ensure that federal employees understand the vulnerabilities of Internet of Things (IoT) devices like smart watches, home appliances, and cars.

Expand the CDM model to critical infrastructure and to the states.

The CDM model, which uses AWARE scores to compare cybersecurity levels among federal agencies, would be an excellent model for U.S. states. CISA could allow states to opt into a program in which CISA provides reviews and recommendations for states' security. If it were equipped with significantly more funding and manpower, it could do the same with critical infrastructure entities.

Establish a standard protocol for how (and when) to get rid of legacy software.

Federal agencies should be prepared for how to get rid of their software before it goes out-of-date.

Create hierarchical requirements for two-factor authentication.

All workers accessing sensitive federal systems should be required to use two-factor authentication (2FA). Users with the most privileged access controls should be required to use 2FA with a physical key, a significantly more secure method than with SMS.

Define America's role in cyber law internationally.

The U.S. should take a more active role in setting cybersecurity standards in the international space. If America doesn't do it, another state will.

Summary

American federal agencies, state and city governments, critical infrastructure companies, and citizens alike rely on internet-connected systems every day to sustain American life as we know it. This trend will only accelerate in the years to come. To deal with our country's persistent cyber vulnerabilities, our leaders in D.C. need to think creatively about solutions that both respect the private sector's autonomy and offer a path toward cohesive cyber preparedness on all fronts.

1 Andersen, M., Perrin, c8eb28bc52b1_story.htmlCybersecurity Challenges Facing the Nation--High Risk Issue. Retrieved from https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary

2 Nyczepir, D. (2019, October 21). House bill would require IoT cybersecurity training for federal employees. Retrieved from https://www.fedscoop.com/iot-cybersecurity-training-federal-employees/
Internet of Things Cyber Security Training for Federal Employees Act, H.R.4774, 116th Cong, 1st session (2019). https://www.congress.gov/bill/116th-congress/house-bill/4774?s=1&r=81

3 Zetter, K. (2014, December 3). An unprecedented look at Stuxnet, the world's first digital weapon. Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

4 Zetter, K. (2011, July 11). How digital detectives deciphered Stuxnet, the most menacing malware in history. Retrieved from https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/

5 Fathi, N. & Broad, W. (2009, February 3). Iran launches satellite in a challenge for Obama. Retrieved from https://www.nytimes.com/2009/02/04/world/middleeast/04iran.html
Spetalnick, M. & Heinrich, M. (2009, September 25). Obama accuses Iran of building secret nuclear plant. Retrieved from https://www.reuters.com/article/us-nuclear-iran-obama-statement/obama-accuses-iran-of-building-secret-nuclear-plant-idUSSUM00011520090925

6 Zetter, K. (2014, December 3). An unprecedented look at Stuxnet, the world's first digital weapon. Retrieved from https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
Nakashima, E. & Warrick, J. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. Retrieved from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

7 Zetter, K. (2014, December 8). Hacker lexicon: what is an air gap? Retrieved from https://www.wired.com/2014/12/hacker-lexicon-air-gap/

8 Greenberg, A. (2019, September 12). New clues show how Russia's grid hackers aimed for physical destruction. Retrieved from https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/

9 Greenberg, A. (2017, December 14). Unprecedented malware targets industrial safety systems in the Middle East. Retrieved from https://www.wired.com/story/triton-malware-targets-industrial-safety-systems-in-the-middle-east/

10 Rapp, N. & Leaf, C. (2019, March 21). How many people work for the U.S. federal government? Retrieved from https://fortune.com/longform/government-employee-count-2019/

11 Koerner, B. (2016, October 23). Inside the cyberattack that shocked the U.S. government. Retrieved from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/
Naylor, B. (2016, June 6). One Year After OPM Data Breach, What Has The Government Learned? Retrieved from https://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned
Perez, E. (2017, August 24). FBI arrests Chinese national connected to malware used in OPM data breach. Retrieved from https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html

12 Hinshaw, D. & Pop, V. (2019, October 25). The Hapless Shakedown Crew That Hacked Trump's Inauguration. Retrieved from https://www.wsj.com/articles/the-hapless-shake-down-crew-that-hacked-trumps-inauguration-11572014333

13 Nakashima, E. & Sonne, P. (2018, June 8). China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. Retrieved from https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html

14 Cybersecurity Challenges Facing the Nation--High Risk Issue. Retrieved from https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary

15 Perez, E. (2017, August 24). FBI arrests Chinese national connected to malware used in OPM data breach. Retrieved from https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html

16 Koerner, B. (2016, October 23). Inside the Cyberattack That Shocked the U.S. Government. Retrieved from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

17 Internet Security Threat Report. (2019, February). Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

18 Mazzei, P. (2019, June 27). Another Hacked Florida Ciyu Pays a Ransom, This Time for $460,000. Retrieved from https://www.nytimes.com/2019/06/27/us/lake-city-florida-ransom-cyberattack.html

19 The Cost of Malicious Cyber Activity to the U.S. Economy. (2018, February). Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

20 Lewis, J. (2018, February 21). Economic Impact of Cybercrime. Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime

21 Hungerford, N. (2019, September 22). Chinese theft of trade secrets on the rise, the US Justice Department warns. Retrieved from https://www.cnbc.com/2019/09/23/chinese-theft-of-trade-secrets-is-on-the-rise-us-doj-warns.html
Rosenbaum, R. (2019, March 1). 1 in 5 corporations say China has stolen their IP within the last year: CNBC CFO Survey. Retrieved from https://www.cnbc.com/2019/02/28/1-in-5-companies-say-china-stole-their-ip-within-the-last-year-cnbc.html

22 Pham, S. (2018, March 23). How much has the US lost from China's IP theft? Retrieved from https://money.cnn.com/2018/03/23/technology/china-us-trump-tariffs-ip-theft/index.html

23 Singer, P.W. and Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York, NY: Oxford University Press USA.

24 Singer, P.W. and Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York, NY: Oxford University Press USA.

25 Schwab, L. (2020, February 6). Interview with Cybersecurity Expert Paul Rosenzweig: The Federal Role. Retrieved from http://newcenter.org/interview-with-cybersecurity-expert-paul-rosenzweig-the-federal-role/

26 What Is the Difference: Viruses, Worms, Trojans, and Bots? Retrieved from https://tools.cisco.com/security/center/resources/virus_differences
What is a computer worm, and how does it work? Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html
What is a computer virus? Retrieved from https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

27 Singer, P.W. and Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York, NY: Oxford University Press USA.

28 Beek, C., Dunton, T., Fokker, J., Grobman, S., Hux, T., Polzer, T., Rivero Lopez, M., Roccia, T., Saavedra-Morales, J., Samani, R., & Sherstobitoff, R. (2019, August). McAfee Labs Threats Report. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

29 Mills, E. (2010, August 25). Bad flash drive caused worst U.S. military breach. Retrieved from https://www.cnet.com/news/bad-flash-drive-caused-worst-u-s-military-breach/

30 Cybersecurity Training & Exercises. Retrieved from https://www.dhs.gov/cisa/cybersecurity-training-exercises

31 Thornton, D. (2019, October 11). NSA develops online cybersecurity course to educate employees, private sector. Retrieved from https://federalnewsnetwork.com/all-news/2019/10/nsa-develops-online-cybersecurity-course-to-educate-employees-private-sector/
Cyber Education and Awareness. Retrieved from https://www.dhs.gov/cisa/cyber-education-and-awareness

32 National Initiative for Cybersecurity Education (NICE). Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/about

33 Smith, A. (2014, November 25). What Internet Users Know about Technology and the Web. Retrieved from https://www.pewresearch.org/internet/2014/11/25/web-iq/

34 Evaluating Information: The Cornerstone of Civic Online Reasoning. (2016, November 22). Retrieved from https://stacks.stanford.edu/file/druid:fv751yt5934/SHEG%20Evaluating%20Information%20Online.pdf

35 Witt, P. (2019, February 28). The top frauds of 2018. Retrieved from https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018

36 Schubert, C. (2020). What is a router, and how does it work? Retrieved from https://us.norton.com/internetsecurity-iot-smarter-home-what-is-router.html

37 Over half of Brits don't change their Wifi password. (2017, July). Retrieved from https://www.reichelt.com/magazin/en/wp-content/uploads/2017/09/Reichelt-WiFi-infographic_UK.pdf

38 Mitchell, B. (2018, October 26). Updated FISMA guidance pressures agencies to use CDM program. Retrieved from https://www.fedscoop.com/cdm-dhs-updated-fisma-guidance-from-omb/

39 Mitchell, B. (2019, May 30). DHS awards $276M contract for CDM dashboard. Retrieved from https://www.fedscoop.com/continuous-diagnostics-mitigation-cdm-dashboard-ecs-federal/

40 Nyczepir, D. (2019, April 26). This agency is preparing to score its cyber risk with a new algorithm. Retrieved from https://www.fedscoop.com/cyber-risk-aware-algorithm/

41 Nyczepir, D. (2019, September 6). CDM's agency cyber risk scores will be relative, at least initially. Retrieved from https://www.fedscoop.com/cdm-scores-relative-kevin-cox-cisa/

42 Mobile Fact Sheet. (2019, June 12). Retrieved from https://www.pewresearch.org/internet/fact-sheet/mobile/

43 Bennetts, M. (2019, December 17). Vladimir Putin 'still uses obsolete Windows XP' despite hacking risk. Retrieved from https://www.theguardian.com/world/2019/dec/17/vladimir-putin-still-uses-obsolete-windows-xp-despite-hacking-risk

44 Hsu, J. (2018, June 4). Why the Military Can't Quit Windows XP. Retrieved from https://slate.com/technology/2018/06/why-the-military-cant-quit-windows-xp.html

45 Two-factor authentication. Retrieved from https://www.login.gov/help/creating-an-account/two-factor-authentication/

46 Two-Step Authentication for Servers and Applications. Retrieved from https://uit.stanford.edu/service/authentication/twostep/servers

47 Shaban, H. (2018, October 8). The government is rolling our 2-factor authentication for federal agency dot-gov domains. Retrieved from https://www.washingtonpost.com/technology/2018/10/08/government-is-rolling-out-factor-authentication-federal-agency-gov-domains/
Yoder, E. (2018, February 27). Central federal jobs site tightens security controls. Retrieved from https://www.washingtonpost.com/news/powerpost/wp/2018/02/26/central-federal-jobs-site-tightens-security-controls/
Cordell, C. (2018, October 9). Rollout of two-factor authentication begins for .gov registrars. Retrieved from https://www.fedscoop.com/gsa-2fa-authentication-dot-gov-websites/

48 Agencies Need to Improve Implementation of Federal Approach to Securing Systems and Protecting Against Intrusions. (2018, December). Retrieved from https://www.gao.gov/assets/700/696104.pdf

49 Vavra, S. (2020, February 5). 500,000 victims pummeled in multi-stage BitBucket malware scheme. Retrieved from https://www.cyberscoop.com/bitbucket-multi-stage-malware-campaign-cybereason/

50 Brandom, R. (2017, July 10). Two-factor authentication is a mess. Retrieved from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

51 Evans, K. & Reeder, F. (2010, November 15). A Human Capital Crisis in Cybersecurity. Retrieved from https://www.csis.org/analysis/human-capital-crisis-cybersecurity

52 Cybersecurity Supply/Demand Heat Map. Retrieved from https://www.cyberseek.org/heatmap.html

53 Nyczepir, D. (2019, April 9). 11 federal agencies help start Cybersecurity Talent Initiative. Retrieved from https://www.fedscoop.com/federal-cybersecurity-talent-initiative/

54 Federal Cyber Reskilling Academy. Retrieved from https://www.cio.gov/programs-and-events/reskilling/
Nyczepir, D. (2019, December 13). As the Cyber Reskilling Academy's second cohort moves on, trainers reflect on the impact. Retrieved from https://www.fedscoop.com/cybersecurity-reskilling-academy-applicant-evaluations/
Cordell, C. (2018, November 30). Cybersecurity Reskilling Academy created by White House for federal employees. Retrieved from https://www.fedscoop.com/cybersecurity-reskilling-program-suzette-kent/

55 Nyczepir, D. (2019, July 31). DHS 'blew up' its hiring system for cybersecurity talent. Retrieved from https://www.fedscoop.com/dhs-cybersecurity-pay-hiring/

56 U.S. Digital Service. Retrieved from https://www.usds.gov/

57 Vavra, S. (2019, November 14). Cyber Command has drastically cut hiring time for cybersecurity roles, says DOD CISO. Retrieved from https://www.cyberscoop.com/cyber-command-hiring-cyber-excepted-service-jack-wilmer/Doe, D. (2019, September 6). Six Strategies for Hiring Tech Talent in Government. Retrieved from https://www.codeforamerica.org/news/six-strategies-for-hiring-tech-talent-in-government

58 Koerner, B. (2016, October 23). Inside the Cyberattack That Shocked the U.S. Government. Retrieved from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

59 Jennings, J. & Nagel, J. (2019, October 24). Federal Workforce Statistics Sources: OPM and OMB. Retrieved from https://crsreports.congress.gov/product/pdf/R/R43590

60 Mellnik, T. & Gregg, A. (2019, January 16). Nearly 10,000 companies contract with shutdown-affected agencies, putting $200 million a week at risk. Retrieved from https://www.washingtonpost.com/graphics/2019/business/contractors-shutdown/
Berry, D. & Collins, M. (2018, December 27). Shutdown puts some programs on hold, but most government agencies continue running. Retrieved from https://www.usatoday.com/story/news/politics/2018/12/27/shutdown-does-not-shutter-all-government-agencies-donald-trump-congress/2422203002/
Nguyen, J. (2019, January 17). The U.S. government is becoming more dependent on contract workers. Retrieved from https://www.marketplace.org/2019/01/17/rise-federal-contractors/

61 Critical Infrastructure Sectors. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors

62 Singer, P.W. and Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York, NY: Oxford University Press USA.

63 Critical Infrastructure Sectors. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors

64 Beek, C., Dunton, T., Fokker, J., Grobman, S., Hux, T., Polzer, T., Rivero Lopez, M., Roccia, T., Saavedra-Morales, J., Samani, R., & Sherstobitoff, R. (2019, August). McAfee Labs Threats Report. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

65 Krebs, C. (2019, December 16). Closing a Critical Gap in Cybersecurity. Retrieved from https://www.lawfareblog.com/closing-critical-gap-cybersecurity

66 The Internet Corporation for Assigned Names and Numbers. (2011, March 4). Beginner's guide to internet protocol (IP) addresses. Retrieved from https://www.icann.org/en/system/files/files/ip-addresses-beginners-guide-04mar11-en.pdf
ExpressVPN. (2020). What is my IP address location? Retrieved from https://www.expressvpn.com/what-is-my-ip

67 U.S. Senate Committee on Homeland Security & Governmental Affairs. (2019, December 12). Sens. Johnson, Hassan introduce CISA ISP subpoena legislation. Retrieved from https://www.hsgac.senate.gov/media/majority-media/sens-johnson-hassan-introduce-cisa-isp-subpoena-legislation

68 Singer, P.W. and Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. New York, NY: Oxford University Press USA.
United States Nuclear Regulatory Commission. (2018, June 21). Backgrounder on the Three Mile Island accident. Retrieved from https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html

69 Schwab, L. (2020, February 6). Interview with cybersecurity expert Paul Rosenzweig: The federal role. Retrieved from http://newcenter.org/interview-with-cybersecurity-expert-paul-rosenzweig-the-federal-role/

70 Nyczepir, D. (2019, July 5). DOE teams with industry on pipeline cybersecurity. Retrieved from https://www.fedscoop.com/doe-industry-pipeline-cybersecurity-recommendations/

71 National Cybersecurity and Communications Integration Center. (2017). NCCIC year in review. Retrieved from https://www.us-cert.gov/sites/default/files/publications/NCCIC_Year_in_Review_2017_Final.pdf

72 National Infrastructure Coordinating Center. Retrieved from https://www.cisa.gov/national-infrastructure-coordinating-center

73 Laudrain, A.P.B. (2018, December 4). Avoiding a world war web: The Paris call for trust and security in cyberspace. Retrieved from https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace Paris call for trust and security in cyberspace. (2018, November 12). Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf?wpisrc=nl_cybersecurity202&wpmm=1 Liste des soutiens a l'appel de Paris. (2018, November 19). Retrieved from https://www.diplomatie.gouv.fr/IMG/pdf/soutien_appel_paris_cle8e5e31-2.pdf

74 Pardes, A. (2018, May 24). What is GDPR and why should you care? Retrieved from https://www.wired.com/story/how-gdpr-affects-you/General Data Protection Regulation. Retrieved from https://gdpr-info.eu/

75 Symantec. (2019). Internet security threat report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

76 Symantec. (2019). Internet security threat report. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

77 Nyczepir, D. (2019, October 21). House bill would require IoT cybersecurity training for federal employees. Retrieved from https://www.fedscoop.com/iot-cybersecurity-training-federal-employees/Internet of Things Cyber Security Training for Federal Employees Act, H.R. 4774, 116th Cong., 1st Sess. (2019).