CYBER READINESS
INSTITUTE

The Urgent Need to Strengthen the Cyber Readiness of Small and Medium-Sized Businesses

A Proposal for the Biden Administration

"As the world becomes more immersed in and dependent on the information revolution, the pace of intrusions, disruptions, manipulations, and thefts also quickens. Technological advancement is outpacing security and will continue to do so unless we change how we approach and implement cybersecurity strategies and practices. Recent attacks in which everyday consumer devices were compromised for malicious use have made it abundantly clear that we now live in a much more interdependent world."

— Commission on Enhancing National Cybersecurity, Report on Securing and Growing the Digital Economy, December 1, 2016

Nearly five years later, those words continue to ring true. We remain mired in a nightmarish game of Whack-A-Mole with our cyber adversaries. But now the digital landscape is larger, and we have no idea where the next cyber attack will pop up. What we know with certainty is that it will. The discovery of major adversary actions, through the SolarWinds and Microsoft Exchange compromises, comes as we emerge from a pandemic year of remote business operations that saw a dramatic rise in ransomware attacks against hospitals, schools, and other critical infrastructure. We are at an inflection point and there is urgent need for action.

info@cyberreadinessinstitute.org

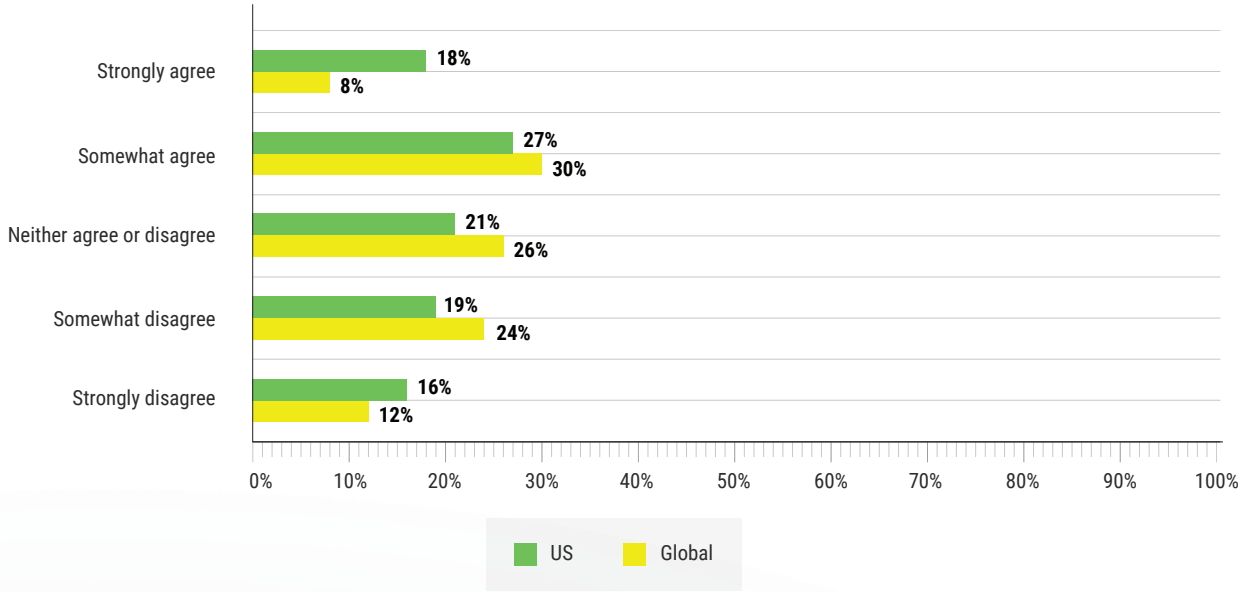
Shockingly expansive and sophisticated, the SolarWinds and Microsoft Exchange events were merely symptoms of the challenges we face. Remedial efforts such as updating and patching our software, changing passwords, and removing malicious code are not sufficient. We must acknowledge and address our failure to incentivize secure behaviors and enact the policies necessary to strengthen our cyber defenses, to make our nation cyber ready.

The SolarWinds and Microsoft Exchange events compromised scores of small and medium-sized businesses (SMBs) that form vital links in our nation's supply chains and economy. SMBs are targeted by cyber attackers because they often lack the resources to invest in cybersecurity tools and training. The intent of this White Paper is to provide the Biden Administration with specific actions to improve the resilience and cyber readiness of U.S. SMBs.

Although we cannot end cyber intrusions, there are basic actions we can take to protect our citizens, businesses, and critical infrastructure. By focusing on the role human behavior plays in successful hacks and by giving SMBs the tools and resources to improve their cyber readiness, we can build a strong and resilient foundation for cybersecurity.

We can also help foster business strength and survival. Given that 60% of SMBs will close their doors within one year of a cyber breach, according to the National Cyber Security Alliance, it is vital to SMBs, and to all of us, that they become cyber aware and ready.

Only 18% of U.S. SMBs are confident ("strongly agree") their organization is prepared for a cyber incident.



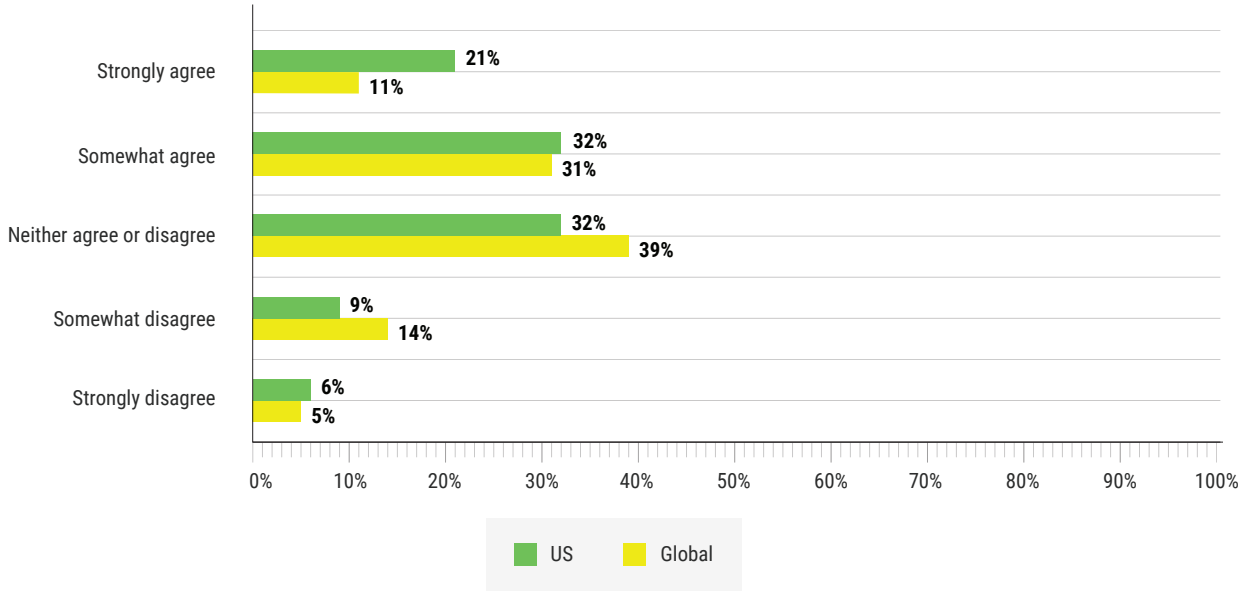
Question: To what extent do you agree that your organization is prepared for a cyber incident and would know how to respond?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

Cybersecurity Landscape and Challenges

The COVID-19 pandemic set off a global rush to enable remote operations by workers, companies, and government agencies. While business and society will benefit from this digital transformation, it has increased vulnerabilities worldwide and across all industry sectors. Nowhere is our exposure greater than among SMBs. Yet, many SMBs do not have the financial resources or human talent for addressing cybersecurity challenges and see little return on investment from spending scarce resources on cybersecurity. According to a 2021 CRI study, only 21% of SMBs are confident that the time and money their organization invests in cybersecurity will decrease their risk. Most SMBs are much more uncertain about the value of investing in cybersecurity. Meanwhile, many large organizations do not even have basic cybersecurity requirements in place for their SMB suppliers or are just beginning to address the issue.

Only 21% of U.S. SMBs are confident ("strongly agree") the time and money invested in cybersecurity decreases their risk.

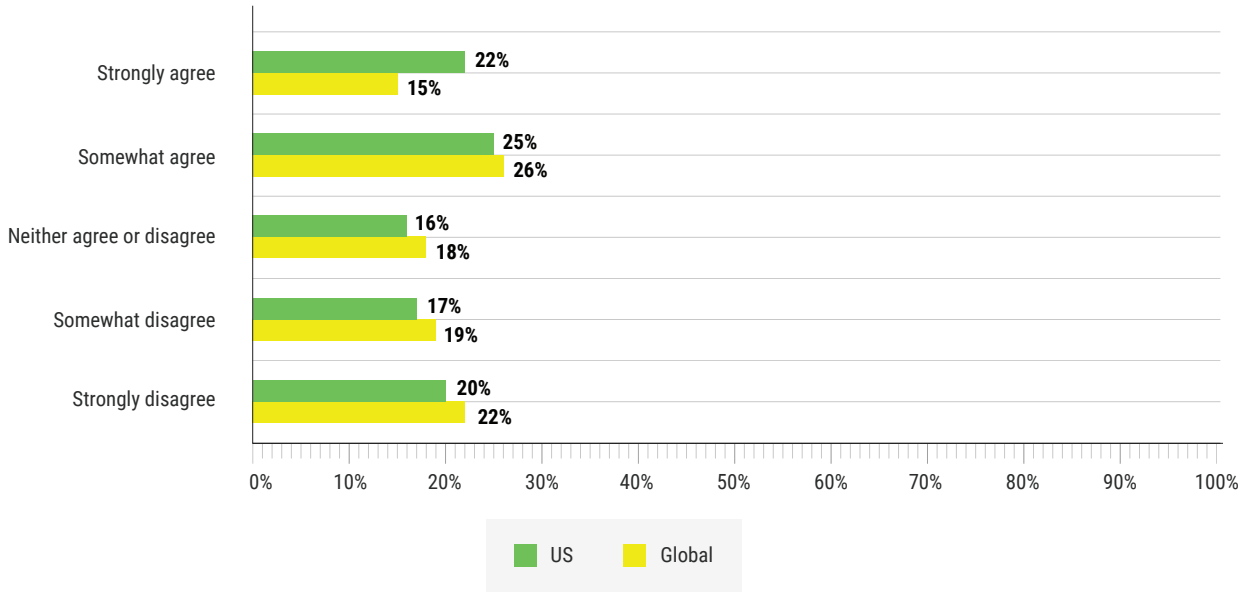


Question: To what extent do you agree that the time and money your organization invests in cybersecurity are decreasing your risk?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

There are multiple threats to SMBs, but ransomware, phishing, and credential-stealing (password theft) are among the most serious. These threats are only expected to grow as industries continue to take all operations online because of the COVID-19 pandemic and the changing nature of work. This rapid change has led to gaps in cyber resiliency, as firms, especially those with fewer resources, struggle to keep up. These increasing vulnerabilities are being readily and frequently exploited by malicious actors.

Only 22% of U.S. SMBs are confident ("strongly agree") they have an employee or team of employees with clear responsibility for cybersecurity.



Question: To what extent do you agree with the following statement: "We have an employee or team of employees with clear responsibility for our cybersecurity"?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

The consequences of a cybersecurity compromise are not only relevant for the company in question but expose other businesses in their supply chain, as well. Given that over two-thirds of large businesses outsource a portion of their functions and allow third-party access to their data, insufficient cyber protection among SMBs can be consequential for larger firms, too. **A 2020 report compiled by Accenture found that up to 40% of cyber breaches are indirect, meaning they target weak links in supply chains or business ecosystems.**

Recommendations

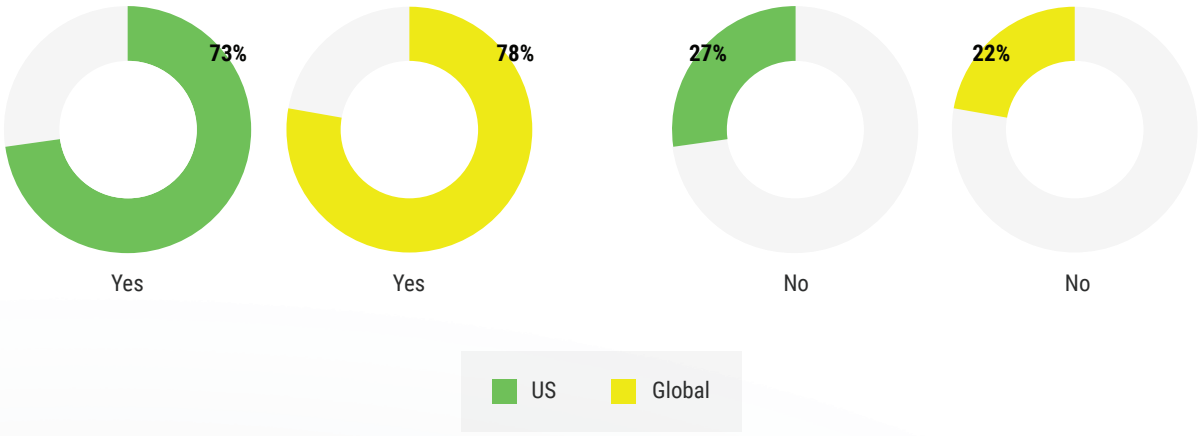
The cybersecurity of U.S. SMBs is integral to the unimpeded operation of our public and private institutions and the economic well-being of our nation. Below are five recommendations to help make U.S. SMBs cyber ready.

- Create a national awareness campaign to promote cyber readiness for SMBs
- Create a cybersecurity resource center for SMBs within the federal government
- Offer tax credits to encourage SMBs to invest in cybersecurity
- Establish public/private collaboration to set minimum standards for cybersecurity
- Create government-funded Cyber Squads, in collaboration with community and 4-year colleges

Create a national awareness campaign to promote cyber readiness for SMBs

As a nation, we have a long history of using public awareness campaigns to save lives and change behaviors—from forest fires to seatbelt safety, to the post-9/11 "See Something, Say Something" advertisements. Now is the time for a national awareness campaign that focuses on the role of human behavior in cybersecurity and educates everyone about the actions that will make us all secure. There is public support for a government campaign: More than 60% of the U.S. and global SMBs, in a 2021 CRI survey, believe the government should create a national public awareness campaign to promote cyber readiness.

Over 70% of U.S. SMBs want the government to do more to help make organizations in the supply chain cyber ready



Question: Should the government offer more support to help you improve the cybersecurity of your organization and others in the supply chain?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

info@cyberreadinessinstitute.org

Cybersecurity is a complex area, not easily reduced to a simple message. An effective public service campaign should focus on a single, basic cybersecurity issue – such as using strong passwords. Focusing on a single topic with a simple recurring message will help protect SMBs from one of the methods favored by hackers.

Create a cybersecurity resource center for SMBs within the federal government

A national awareness campaign focused on cyber readiness will naturally direct SMBs to a list of available public and private resources. Today, those resources are scattered across several government agencies, sometimes with advice that is too technical for many business owners who do not have an internal IT staff or who outsource cybersecurity. Given the ongoing work for SMBs by the Cybersecurity and Infrastructure Security Agency (CISA), we recommend that CISA is the agency best positioned to be tasked with the curation of cybersecurity resources for SMBs. The agency commissioned to curate resources must also have as its core mission the task of simplifying concepts surrounding cybersecurity to make them understandable and accessible to business owners.

Offer tax credits to encourage SMBs to invest in cybersecurity

To spur SMB investments in cybersecurity, the federal government should provide an incentive in the form of tax credits. The Treasury Department, in collaboration with the Small Business Administration (SBA) and CISA, should establish guidelines for SMB investment in cybersecurity to qualify for tax credits. While tax credits will reduce the amount of taxable income the government collects, improved cybersecurity will reduce the economic damage done by cyber attackers and have a net positive impact on the security, strength, and resilience of the digital economy.

Working with other agencies and soliciting industry input, Treasury can establish requirements for companies to indicate that they have taken steps to become cyber ready before receiving any tax credit. These standards should require cybersecurity training and education for employees to qualify for the credit. Education should underscore the need to create a culture of cybersecurity in the workplace. Awareness of the risks that come with cyber breaches, and behaviors that mitigate these risks, should be embedded in everyone's actions, from employees to firm leadership so that employees understand their responsibilities, and actions are taken to ensure the organization is cyber ready.

Establish public/private collaboration to set minimum standards for cybersecurity

We can no longer rely on market forces or voluntary actions to improve the cybersecurity of our public and private institutions. Currently, “first-to-market” trumps “secure-to-market.” Market forces prioritize profit over security – and enable vulnerabilities, which our adversaries easily expose. This structure is unacceptable and must change. We must create standards that prioritize security in the market. Aligned with an effective education and awareness campaign, market standards for security will help consumers prioritize security, as well.

Establishing standards through industry and government collaboration is vital to securing supply chains. We have successfully established regulations that improve the safety of our roads, health care, and financial systems. We should establish minimum standards for cybersecurity.

There is no one-size-fits-all solution to preparing organizations to be cyber ready. The number of employees, industry, technical knowledge, and financial capabilities are just a few factors that vary by company. But industry and government can work together to establish standards, focused on a risk management approach, that take those factors into account.

Create government-funded Cyber Squads, in collaboration with community and 4-year colleges

A government program funded through grants awarded by the National Science Foundation already exists—CyberCorps: Scholarship for Service. That program, however, is designed to recruit and train IT professionals and cybersecurity managers for positions with federal, state, and local agencies. A new Cyber Squad program would expand the pipeline of talent available to SMBs and will also facilitate engaging different disciplines and expertise in creating cultures of cyber readiness across SMBs.

Cyber Squads can address several issues that hinder SMB efforts to become cyber ready— including a talent shortage and a lack of financial resources. A Cyber Squad program modeled after the Peace Corps or a campaign similar to the Science, Technology, Engineering, and Mathematics (S.T.E.M.) education initiative will allow students to explore an interest in pursuing cybersecurity as a career path while providing a connection with their local communities.

In cooperation with community colleges and universities, student interns with expertise in various disciplines would receive additional training in the role human behavior plays in making SMBs secure—issues such as password management, updating software, and phishing awareness—that are not addressed in many cybersecurity programs. Cyber Squads would be sent into the community to help local SMBs improve their cyber readiness. Initially, the program would focus on helping underfunded minority-owned businesses.

Conclusion

These recommendations and actions highlight the need for urgent public/private collaboration to address the serious vulnerabilities that put our national security and economic well-being at risk. **Now, more than ever, we need proactive, deliberate collaboration and collective action between government and industry.**

The cyber events of the last year demonstrate how our cyber adversaries are increasingly sophisticated in identifying our vulnerabilities and weaknesses and exploiting them. We must bolster our cyber defensive capabilities while continuing to invest in our offense.

SMBs need access to cybersecurity resources that are prescriptive and accessible. Resources, tools, and techniques for SMBs require a different approach from what larger enterprises need. The goal is the same, to create a healthy protected company, but the path to get there is different. We cannot simply shrink the tools and techniques employed by major corporations into smaller versions for SMBs.

We must be proactive in supporting SMBs to become a strength in our ecosystem, not a weakness. They must become more resilient and cyber ready to ensure our nation has a strong foundation and a culture of security.

About the Cyber Readiness Institute

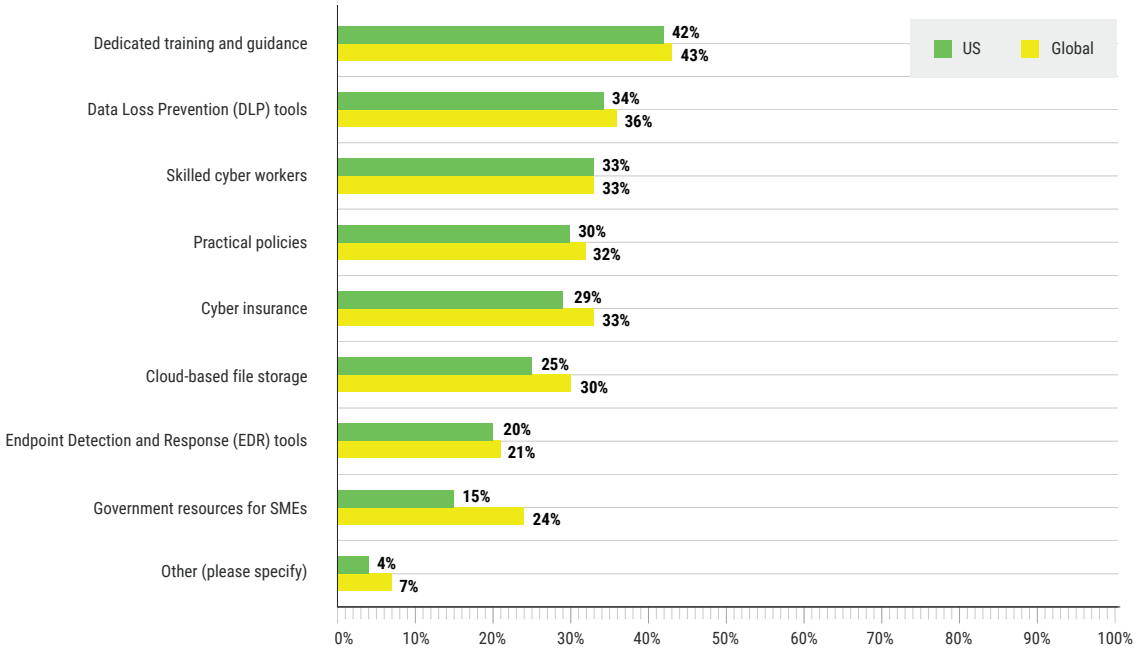
CYBER READINESS INSTITUTE

The Cyber Readiness Institute is a non-profit initiative that convenes business leaders from across sectors and geographic regions to share resources and knowledge that inform the development of free cybersecurity tools for small and medium-sized businesses (SMBs). CRI was co-founded by the CEOs of The Center for Global Enterprise, Mastercard, Microsoft, PSP Partners, as a follow-up action from the work of the Commission on Enhancing National Cybersecurity. Our members also include ExxonMobil, General Motors, and Principal. Our mission is to advance the cyber readiness of SMBs to improve the security of global supply chains. CRI's resources focus on human behavior and emphasize employee education and awareness. To find out more, visit www.BeCyberReady.com.

Appendix

Cyber Readiness Institute Global Cybersecurity Survey*, January 2021

Most SMBs need dedicated training and guidance to make their organization more cyber-secure.

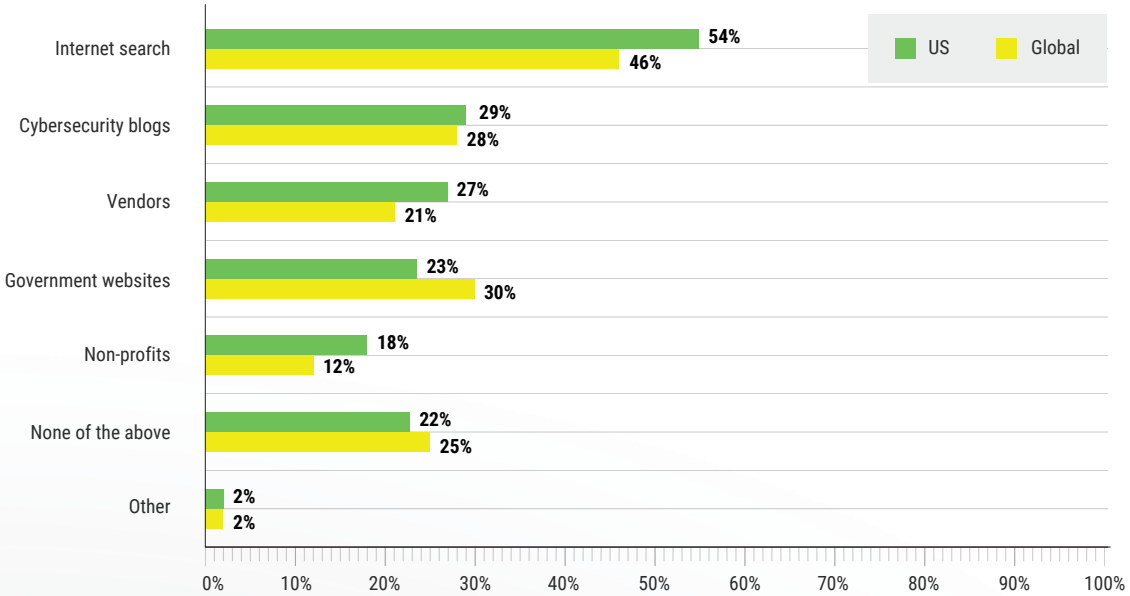


Question: Which of the following do you need to make your organization more secure? (select all that apply)

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

**Survey Size: U.S. is 576 and Global is 517*

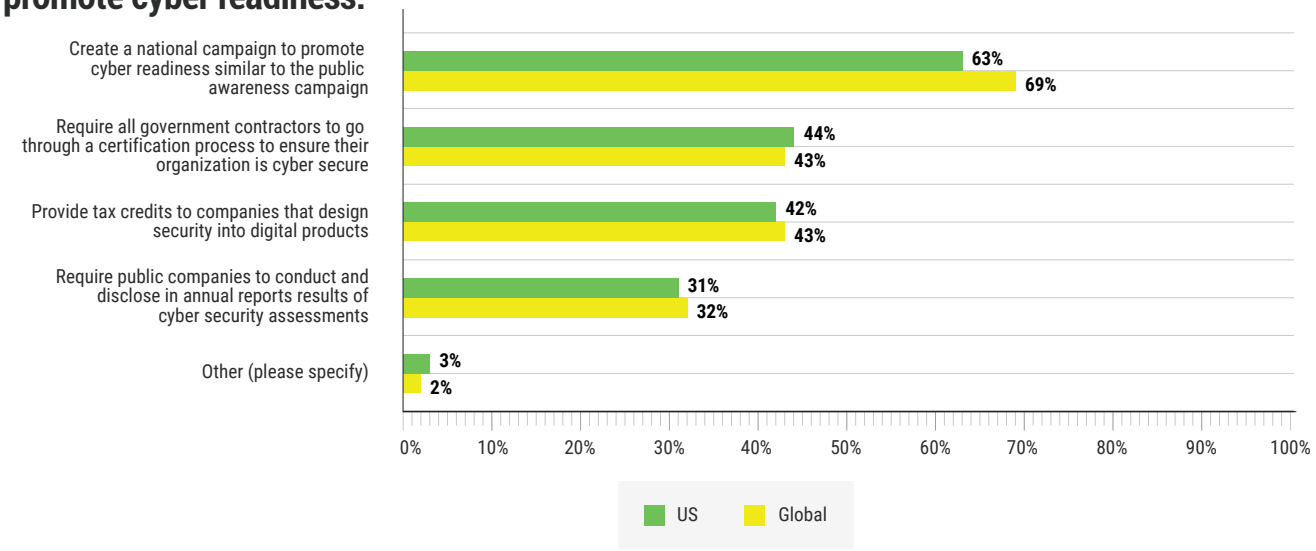
Most SMBs rely on Internet searches to find cybersecurity resources.



Question: Which of the following sources have you visited to find cybersecurity resources for your organization?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

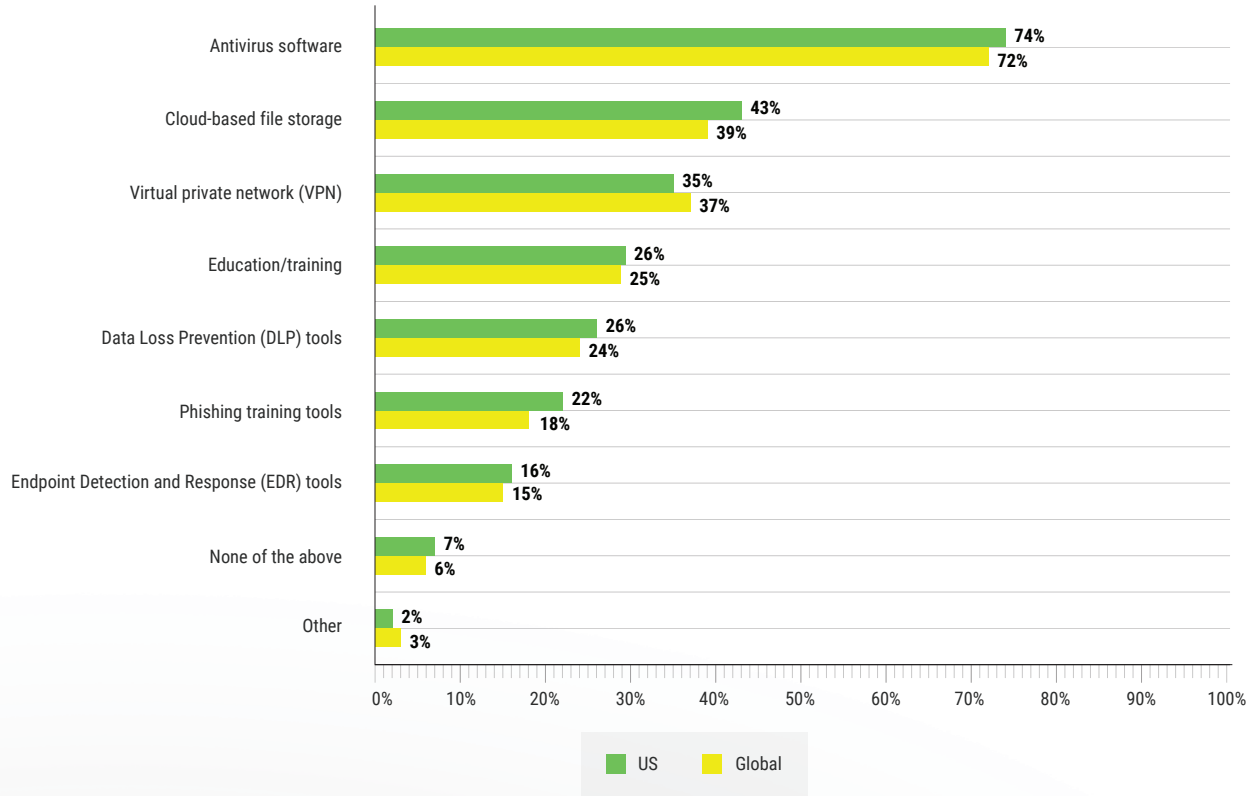
Over 60% of U.S. SMBs want the government to create a national awareness campaign to promote cyber readiness.



Question: Which of the following steps should the government take?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

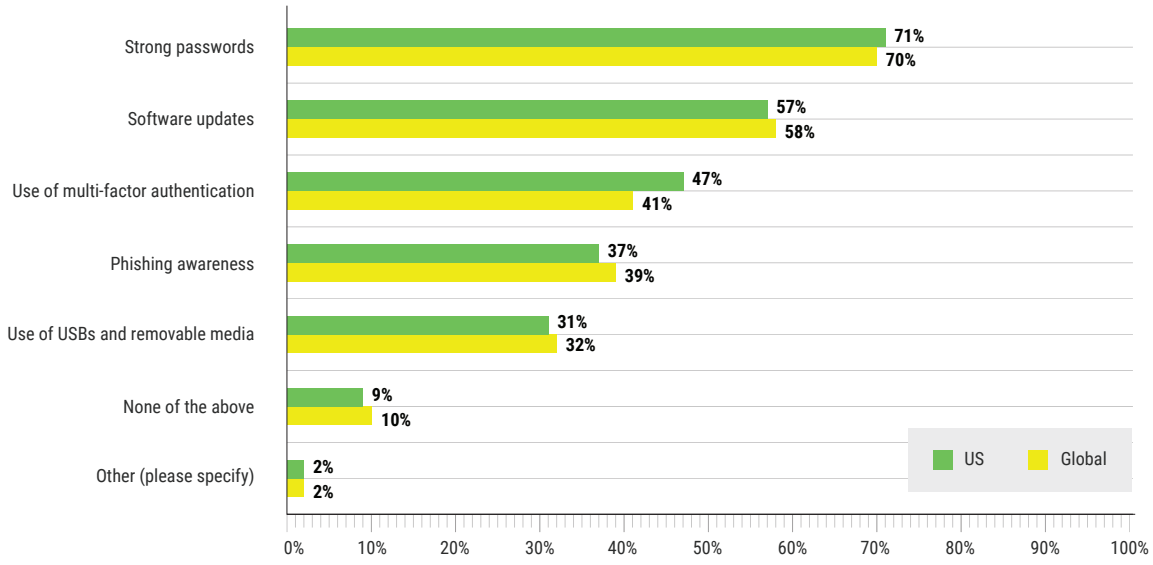
Antivirus software, cloud-based file storage, and virtual private network (VPN) are the top three cybersecurity tools SMBs rely on.



Question: Which of the following technologies and/or tools have you used to help keep your organization cyber secure?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

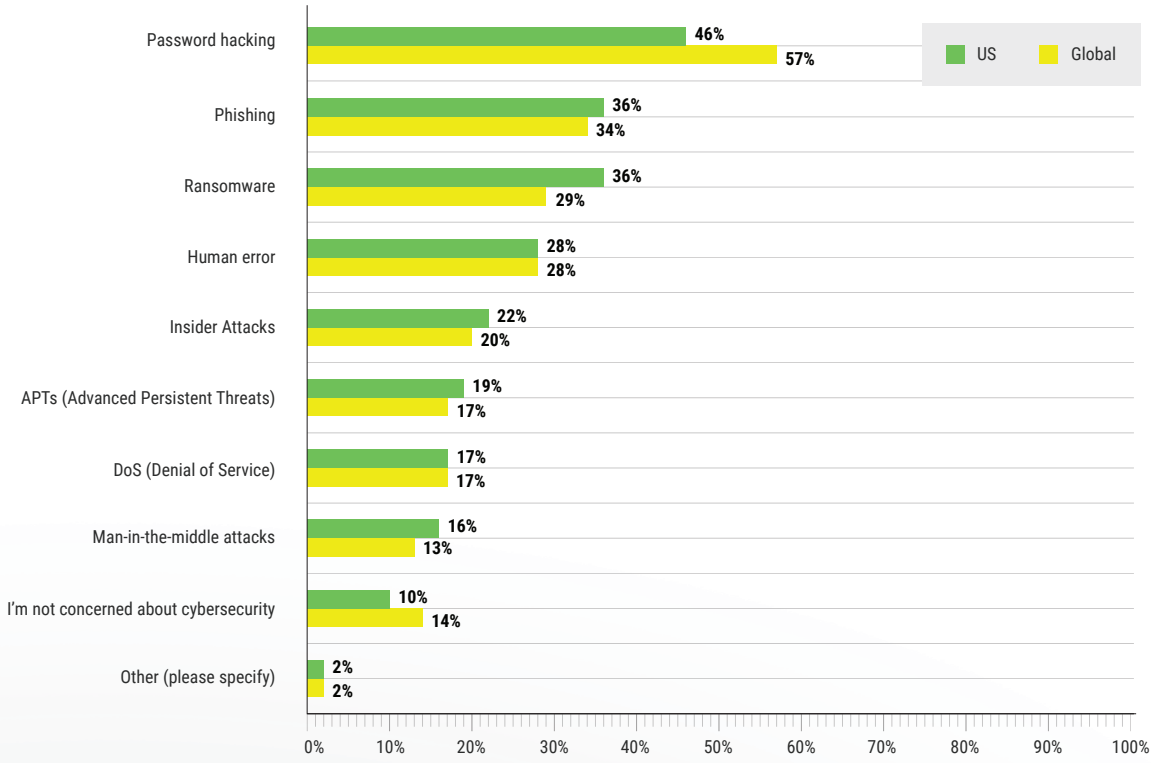
71% of U.S. SMBs say their employees are trained to use strong passwords. BUT weak passwords are still the primary reason for recent hacks.



Question: Which of the following cybersecurity-related topics are employees at your organization trained to address?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021

Password hacking tops the list of cybersecurity concerns among SMBs, along with phishing, ransomware, and human error.



Question: What are you most concerned about regarding the cybersecurity of your organization?

Source: Cyber Readiness Institute Global Survey, Small and Medium-sized Businesses, January 2021