ACT | The App Association

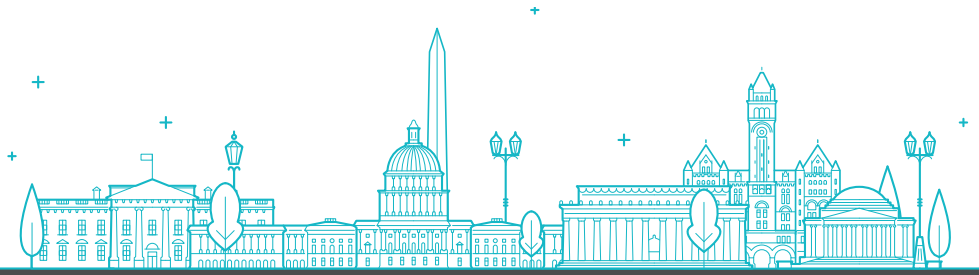
Strengthening the Cybersecurity Posture of America's Small Business Community

Testimony of

Graham Dufault
Senior Director for Public Policy
ACT | The App Association

Before the

U.S. House of Representatives
Small Business Committee



1401 K Street NW Suite 501
Washington, DC 20005
202.331.2130
www. ACTonline.org
@ACTonline
/ACTonline.org

Executive Summary

ACT | The App Association (the App Association) is the leading trade group representing small mobile software and connected device companies in the app economy, a $1.7 trillion ecosystem led by U.S. companies and employing 301,030 people in New York and 88,190 people in Missouri.[1] Our member companies create the software that brings your smart devices to life. They also make the connected devices that are revolutionizing healthcare, education, public safety, and virtually all industry verticals. They propel the data-driven evolution of these industries and compete with each other and larger firms in a variety of ways, including on privacy and security protections.

We applaud this Committee for examining the impacts of cyber threats and what Congress can do to ameliorate the cybersecurity posture of small businesses. In recent months, the United States has faced serious cyber incidents targeting a range of victims and through a variety of attack vectors. We can learn much from these incidents, and they should inform the Committee's work in the 117th Congress to equip small businesses with the tools they need to keep Americans safe from cyberattacks. Our message to the Committee is simple and has four components:

- Recent attacks highlight the importance of timely and appropriate disclosure of a cyber incident as well as a strong infrastructure for threat and defensive measure sharing to investigate bad actors. Congress can do more to promote information sharing of threats and defenses—especially for small businesses.
    - For example, we supported previous efforts by this Committee (H.R. 1648 and 1649, 116th)[2] to provide Small Business Administration (SBA) cyber expertise and establish an information sharing channel especially for small businesses.

- Software platforms (app store / operating system combinations) and cloud services play a key role in our cybersecurity posture in the mobile and desktop space; app makers leverage the security features and controls they provide.

- Federal policies should continue to promote the use of technical protection measures (TPMs) like end-to-end and device encryption.

- App Association members suffer from a lack of available software personnel, with about 3.5 million unfilled cybersecurity jobs globally, according to one estimate.[3] We support significant federal investments in workforce development to produce

[1] ACT | THE APP ASSOCIATION, STATE OF THE U.S. APP ECONOMY: 2020 (7th Ed.), *available at* https://actonline.org/wp-content/uploads/2020-App-economy-Report.pdf.
[2] Small Business Advanced Cybersecurity Enhancements Act of 2019 (H.R. 1648, 116th); Small Business Development Center Cyber Training Act of 2019 (H.R. 1649, 116th).
[3] 2019/2020 OFFICIAL ANNUAL CYBERSECURITY JOBS REPORT, CYBERSECURITY VENTURES (2021), *available at* https://cybersecurityventures.com/jobs/.

software developers and cybersecurity experts who can meet and exceed today's cybersecurity challenges.

I. Recent Attacks Underscore the Need for Federal Assistance on Cybersecurity

Recent successful ransomware attacks have underscored the need for this Committee to review its role in bolstering cybersecurity for small businesses. For example, on July 2, 2021, hackers associated with REvil exploited a vulnerability in Kaseya's IT management system, Virtual System Administrator (VSA), to perpetrate a massive ransomware heist snaring about 1,500 businesses. Interestingly, Kaseya had almost prevented the incident. On April 1, Dutch Institute for Vulnerability Disclosure identified seven vulnerabilities in VSA, and Kaseya successfully patched four of them before hackers took advantage of one of the remaining three. Although the attack mainly targeted a large firm with lots of clients, many of the impacted businesses are small companies that are either partners that resell Kaseya offerings and provide services around them or are clients of Kaseya.

Small companies have a built-in incentive to protect themselves from cyberattacks like those involving ransomware. Even if a small business can afford to pay the ransom itself, the cost of remediating after an attack can be crippling.[4] And if the financial fallout directly resulting from an attack does not kill a small company, the reputational damage could. Customers went back to Target after its breach, but the same perhaps could not be said for customers of little-known app makers. For small companies, the consequences of an attack can be dire, and they present ample motivation not to be the weak link in any digital supply chain.

a. Information Sharing Challenges

Enhancing information sharing by small businesses is especially important because smaller companies are a favorite target of cyber criminals. Reports suggest that up to 71 percent of cyberattack targets are small companies.[5] Several of our member companies have shared stories about phishing scams and similar attacks, and the App Association itself is an occasional target of social engineering. The fact that a business is small should not prevent it from sharing key information about the attack with those who can make use of it. If they fail to do so, we could be missing a substantial piece of the investigative puzzle. Cyber threats evolve quickly and developing a robust understanding about how cyber criminals design their attacks for various kinds of targets in real-time is a key component to a successful national cyber policy. As Joe Bonnell, founder and CEO of our member company Alchemy Security in Denver, CO,

---

[4] INST. FOR SECURITY AND TECH., RANSOMWARE TASK FORCE, COMBATING RANSOMWARE (Jun. 2021), *available at* https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.

[5] BEAZLEY, 2019 BREACH BRIEFING 8 (2019), *available at* https://www.beazley.com/documents/2019/beazley-breach-briefing-2019.pdf.

tells us: if anyone in the cybersecurity business took a three-month hiatus, they would have to relearn everything they knew completely. Information sharing and the advanced tools to make it useful are necessary to match the speed of the enemy.

As former Cybersecurity and Infrastructure Security Agency (CISA) Director Chris Krebs recently pointed out, ransomware (like many forms of cybercrime) is a business.[6] Federal policy should therefore focus on prioritizing enforcement to deter ransomware attacks, increasing costs for cybercriminals, while also lowering their expected returns on investment by better preparing government and private sector actors to respond. One key aspect of deterrence and enforcement is empowering all relevant stakeholders to share what they believe to be threat information in a format that works for investigators and in a manner that does not expose sharing entities to undue liability. Threat sharing for smaller companies is complicated, however.

The Department of Homeland Security (DHS) has shared and facilitated cyber threat data sharing for years. But the structure and mechanics of information sharing are complicated. The main private sector information sharing hub, United States Computer Emergency Readiness Team (US-CERT) is a 2003 outgrowth of DHS' Office of Cybersecurity and Communications (CS&C). Now US-CERT is the triage and information sharing branch of CS&C's National Cybersecurity and Communications Integration Center (NCCIC), which is now, as of 2018, a subdivision of the Cybersecurity and Infrastructure Security Administration (CISA). But it is DHS' Office of Intelligence and Analysis (I&A) that deploys field personnel to support the National Network of Fusion Centers (National Network), which accepts and shares threat data at the local level. The portals for private sector entities to receive and share threat data are often private sector-led information sharing and analysis centers (ISACs). However, small and medium enterprises (SMEs) usually lack the resources and wherewithal to join and participate regularly in ISACs. Moreover, most ISACs serve critical infrastructure industries, and most of our members fall outside the definition of critical infrastructure.

So, which arbitrary arrangement of alphabet soup is most important to a small business? When an App Association member company is hit with a cyberattack, whom do they share it with? Somebody at NCCIC? Somebody at their local Fusion Center or an ISAC? Where are these entities, and how should our companies share threat information with them? As with specialized legal and accounting functions, small businesses cannot be expected to maintain in-house cybersecurity expertise. But as Sebastian Holst, chief operating officer of our member company vFortified, points out, while small companies may be able to contract with IT firms to outsource cybersecurity services, they cannot transfer away cybersecurity risks from their business or outsource their own accountability. Sebastian also notes that we cannot expect small businesses to be able to effectively select and leverage outside cybersecurity firms without first

---

[6] Hearing on "Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis," before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, & Innovation (May 5, 2021), 117th Cong., 1st Sess. (Statement of Christopher C. Krebs 3-4), *available at* https://homeland.house.gov/imo/media/doc/2021-05-05-CIPI-HRG-Testimony-Krebs.pdf.

having their own independent, working knowledge of cyber threats and information sharing best practices. Small companies will always have ultimate responsibility for the fallout from cybersecurity attacks and, as such, will always suffer the inevitable financial and reputational consequences that follow. And yet, about 83 percent of small companies report that they do not have the capabilities to manage cyber risks. Organizations like the Cyber Readiness Institute provide meaningful materials for small businesses and there is a role for government as well. If federal outreach can help simplify and streamline the learning curve for non-expert small companies, they will be in a better position to secure their businesses, their partners, and of course their customers. Improving small company awareness brings us further down the road to improving information sharing overall to better protect our local economies from threats both here and abroad.

b. Legislative Proposals to Address the Challenges

We commend this Committee for moving legislation in past Congresses to address these issues. Specifically, the Committee unanimously approved H.R. 1648 and H.R. 1649 last Congress. We appreciate that H.R. 1648 designates a single federal entity, the Small Business Administration (SBA), as the information sharing hub for small businesses based in the United States that are not otherwise under a separate information sharing framework. The legislation also appropriately collocates the central Small Business Cybersecurity Assistance Unit (SBCAU) with the existing National Cybersecurity and Communications Integration Center (NCCIC), enabling the agencies to work closely together on the common goal of facilitating threat indicator and defensive measure sharing. The bill also builds on the Cybersecurity Information Sharing Act of 2015's liability protections, clarifying that small businesses sharing covered information with SBCAU are not liable for causes of action arising from actions or inactions associated with sharing such information. If a hacker tries to use a novel behavioral engineering attack on one of our member companies—for example, a specific type of phishing email or communication—the bill would provide an incentive for them to share the relevant information with SBCAU. Investigators could match the attempt with others like it, and it may be the missing piece to prosecute the perpetrators or take other measures to stop them.

Beyond information sharing, H.R. 1648 also bolsters cybersecurity resource materials for small business concerns, including by requiring SBA to coordinate with National Institute for Standards and Technology (NIST) to identify and disseminate information on the most cost-effective methods of implementing the NIST cybersecurity framework; and requiring SBA's Office of Advocacy to ensure that other agencies avoid compromising the cybersecurity posture of small business concerns. The NIST Cybersecurity Framework provides a useful guide for companies to operationalize the management of cyber risk. But Version 1.0 of the Framework is 41 pages, and Version 1.1 is longer, at 55 pages. Small businesses, even in tech-driven sectors like our members, have precious little time and resources to get through dense documents that recommend consultation of more resources—such as "COBIT 5 BAI09.01, BAI09.02,"[7]

[7] Nat'l Inst. Of Standards and Tech, Framework for Improving Critical Infrastructure Cybersecurity 24 (Apr. 16, 2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

which provides a system for the inventory of physical devices and systems. Although the Framework is intended to be scalable for SMEs, its complexity is daunting, and the provisions of H.R. 1649 tailoring NIST's and similar materials for small companies is a welcome proposal.

The Committee also took a positive step with H.R. 1649, which would require SBA to create a certification program to certify some of its own employees as cyber counselors. The bill would house the counselors in regional Small Business Development Centers (SBDCs) and require SBDCs to maintain a minimum threshold percentage of staff with cyber counselor certification. Rob Pope, the co-founder and chief technology officer of App Association member Dogtown Media, supports this concept, noting that the majority of small businesses he has worked with recently have no full-time IT staff. He also points out that they are generally confused by available cybersecurity guidance, including the NIST framework. As this Committee and others take steps to enhance federal protections and resources for companies to improve their cybersecurity capabilities, spreading the word about these enhancements is another challenge, and certifying SBA employees in SBDCs can go some distance toward addressing the problem. The bill is a good complement to H.R. 1648 because having cyber experts in the SBDCs can help ensure that small companies across the nation are actually making use of the incentives and information sharing structure in H.R. 1648.

II. Software Platforms and Cloud Services Play a Key Role in Small Business' Cybersecurity Posture

As app makers, our member companies benefit from leveraging the security features in mobile devices and their operating systems, as well as through app store vetting. Our member companies purchase a bundle of services from software platforms—the app store / operating system combination—and that bundle includes security features. For example, app stores currently vet apps for security flaws and facilitate the general distribution of software updates to apps' users. The vetting function is a worthwhile hurdle our member companies clear because it creates an environment in which consumers trust the apps in the store, even when they come from app makers they have never heard of—the common profile of our member companies. Similarly, mobile operating systems generally reject "sideloaded" software that an app store has not vetted and which may contain malware or other defects. Android allows consumers to install unapproved apps, but only if the consumer expressly authorizes installation from a specific source in the device's settings, while Apple's iOS completely disallows unapproved software on the operating system.[8] These are important measures to

[8] Dallas Thomas, "How to Sideload Apps by Enabling 'Unknown Sources' or 'Install Unknown Apps,'" GADGET HACKS (Jan. 24, 2020), *available at* https://android.gadgethacks.com/how-to/android-101-sideload-apps-by-enabling-unknown-sources-install-unknown-apps-0161947/.

protect consumers and enhance App Association member prospects by bringing consumers to the marketplace.

The measures software platforms take to prevent cyber incidents are not based on theoretical risks. Ransomware has migrated to mobile platforms in the form of locker ransomware, which locks a mobile device's user interface and only unlocks upon payment of the ransom. The typical attack involves clickbait or another kind of link that, if clicked, downloads the ransomware onto an Android device.[9] Another observed method is for bad actors to create fake versions of popular apps like Netflix and Candy Crush, entice consumers to sideload them, and use them to circumvent operating system permissions to spy on their targets. These copycat apps have been known to take control of microphones, take screen shots, log keystrokes to steal credentials, and even access messages, contacts, and location.[10] If the device is running a recent version of Android, the attack vectors are limited to sources (e.g., the Chrome browser) the consumer expressly authorized to download software that Google Play has not approved. In the case of iOS, these attack vectors are mainly limited to trying to sneak malicious code by app reviewers because the option to allow sideloading from a specific source is not available.

The ability for software platforms to narrow or close these kinds of attack vectors is crucial to a strong cybersecurity posture for small companies doing business in the mobile space. This is especially true because the worst threats are overseas and outside United States jurisdiction, where they are beyond the reach of federal penalties. Since Congress cannot legislate away this downside risk, it is even more important to empower private sector actors to employ gating practices to protect consumers on smart devices from foreign threats. Therefore, we oppose proposals like the American Choice and Innovation Online Act (H.R. 3816), which would prohibit some of the measures software platforms take to limit attacks on consumers because they could be said to advantage the platform's own offerings over others by limiting free access to consumer data and device and operating system features to all comers. One of the consequences of legislation removing the gating function software platforms provide is to put the onus on consumers to figure out whether they should trust software makers. This result would be highly disruptive to App Association member prospects; in general, consumers are not familiar with small app makers, which do not have the built-in consumer trust large, established brands have. If consumers can trust the app stores and operating systems to prevent malware, consumers are much more likely to download software from a company they've never encountered. Conversely, consumers may generally stop downloading software from unknown companies if they are unable to rely on the app stores and operating systems to prevent and remove malware. We urge the members of this Committee to view proposals like H.R. 3816 with skepticism

---

[9] Jaime-Heather Schwartz, "How to protect your Android phone from ransomware – plus a guide to removing it," AVIRA (Aug. 13, 2020), *available at* https://www.avira.com/en/blog/ransomware-android-phones.

[10] Danny Palmer, "This Android trojan malware is using fake apps to infect smartphones, steal bank details," ZDNET (June 1, 2021); Lindsey O'Donnell, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks," THREATPOST (April 21, 2020); Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World," CYBEREASON (July 1, 2020).

on the grounds that they would harm the cybersecurity posture and business prospects of small mobile software and connected device companies.

Small firms also leverage the cybersecurity capabilities of cloud services to better protect themselves. As Microsoft president Brad Smith pointed out in February in his testimony on SolarWinds, cloud hosting (as opposed to maintaining on-premises servers) enables better situational awareness and defense measures, especially against the routine—yet recently effective—components of an attack designed to gain incrementally greater levels of access.[11] For example, in the SolarWinds breach, Russian attackers gained access to some credentials by using a "password spray" approach, where attackers try a couple of common passwords on a high volume of accounts. This way, they avoid account lockout triggered by multiple attempts on a single target, and the odds are someone in any given organization is using a common password. As Smith points out, "[w]hen Microsoft's cloud services are attacked, we can detect anomalies and indicators of compromise in ways that are not possible in an on-premises environment."[12] Although on-premises servers are not necessarily inherently less secure, it is simply more resource-intensive to maintain robust cybersecurity protections around them, especially for small companies. For many of them, migrating to cloud services has provided access to the platform-level intelligence on threat and compromise indicators, as well as real-time patches to vulnerabilities that employees would otherwise have to install on their own with on-premises servers.

III. The Statutory and Regulatory Environment Should Encourage Encryption and Similar Technical Protection Measures

Although encryption is not a complete solution by itself, it is an essential tool, especially for SMEs, to protect data. App makers rely on the trust consumers have in their devices and software. Especially in the mobile space, consumers take their most sensitive data with them everywhere on their secure mobile devices. The ability to encrypt these devices without a third party maintaining a separate key or vulnerability is an important aspect of continuing down the path we are on now to unlock the potential of smart devices to handle our finances, manage our health information, and access work. Mandating that messaging providers build "backdoors" into end-to-end encryption—or that device makers keep separate vulnerabilities for device encryption—for the purposes of government access would degrade the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. The existence of mandated vulnerabilities like these make the business prospects for cyber crime much more attractive. Hackers might spend hours or days

[11] Joint Hearing on "Weathering the Storm: The Role of Private Tech in the SolarWinds Breach and the Ongoing Campaign," before the U.S. House Committee on Homeland Security and the U.S. House Committee on Oversight and Reform (Feb. 26, 2021) (statement of Brad Smith, President and Chief Legal Officer, Microsoft Corp.), *available at* https://homeland.house.gov/imo/media/doc/Testimony-Smith.pdf.
[12] *Id.* at 12.

trying to determine if a vulnerability exists at all and then might give up if they think there is no way in. But if they know it has to exist because the law mandates it, suddenly the resource investment of attacking the service is worth it—eventually someone will discover it.

Occasional calls for "responsible" end-to-end or device encryption are simply not responsible for your constituents and App Association members' customers. This is a lesson we learned with the Clipper chip, which was a mistake that should not be repeated. "Responsible" encryption is just another word for *broken* encryption. In fact, encryption is in many ways a far better tool for crime prevention than investigation. We want to stop the bad guys before they harm your constituents. Not only that, but the federal consensus currently seems to be that strong encryption should either be required or encouraged. The Federal Trade Commission describes encryption of sensitive customer information when transmitting it as a "basic step" to maintain security, confidentiality, and integrity of customer information for financial institutions.[13] Similarly, the Department of Health and Human Services in its Health Insurance Portability and Accountability Act (HIPAA) rules make encryption an "addressable implementation specification" that must be implemented if, "after a risk assessment, the entity has determined that the specification is a reasonable and appropriate safeguard . . ."[14] Weakening encryption to facilitate investigations would also facilitate the success of criminal hackers and limit our ability to keep them out.

IV. Congress Should Continue to Invest in Workforce Development to Expand the Software and Cybersecurity Workforce

Despite providing a median annual salary exceeding $89,000,[15] more than 500,000 computing jobs remain unfilled in America. With just 65,000 U.S. college graduates earning computer science degrees each year on average, recent American graduates are filling a mere fraction of the available computing jobs. Moreover, the number of computer and information technology occupations is projected to grow 11 percent from

[13] Fed. Trade Comm'n, Financial Inst. And Customer Information: Complying with the Safeguards Rule, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[14] U.S. Dep't of Health and Human Svcs., Health Information Privacy FAQs, Is the use of encryption mandatory in the Security Rule?, *available at* https://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html.

[15] Computer and Information Technology Occupations, Occupational Outlook Handbook, US BUREAU OF LABOR STATISTICS, *available at* https://www.bls.gov/ooh/computer-and-information-technology/home.htm

2019 to 2029, much faster than the average for all occupations in the United States—with the number of software developing jobs expected to grow by 22 percent. [16]

That's not to say that some of the solutions to upskilling don't already exist in the private sector: In summer 2020, Microsoft launched its Global Skills Initiative[17] to provide discounted certification exams, technical courses, and online skills courses. As Portia Wu outlined in congressional testimony earlier this year, "Online learning can be a tremendous tool for individuals to gain skills—particularly for those who cannot access education during traditional hours or cannot physically go to learning institutions." The private sector can help, but policymakers must create an environment in which employers and educators can equip those in our current and future workforce with the skills needed to succeed in their jobs. Access to and removing barriers from resources to attain these jobs constitutes a huge part of this effort.

There are several items Congress should consider in supporting the robust development of the American workforce in the 21st century:

- Pass the CHampioning Apprenticeships for New Careers and Employees in TECHnology Act (CHANCE in TECH Act, H.R. 720). This legislation would require the Department of Labor to enter into competitive contracts with intermediaries that manage apprenticeship programs on behalf of employers. By enabling would-be employers to streamline their apprenticeship processes, which many employers need to fully train developers and others, the CHANCE in TECH Act would help connect workers to the employers that need them.

- Appropriate at least $250 million to the science, technology, engineering, and math (STEM) Master Teacher Corps (MTC) program. Our schools' failure to provide computer science courses is rooted in part in a lack of training and professional development for teachers to attain an advanced formal education in teaching computer science. Congress must adequately resource the STEM MTC program to prepare our kids for the jobs of the future and maintain our position as the global leader in tech-driven industries.

- Pass the Computer Science for All Act (H.R. 3602). This legislation would authorize $250 million in new grants to support a diverse tech pipeline in pre-K through grade 12 education. By investing in low-income and underserved communities, the diversity gap in STEM careers can begin to be bridged while encouraging the growth of the next generation of tech talent.

---

[16] Software Developers, Computer and Information Technology Occupations, Occupational Outlook Handbook, US BUREAU OF LABOR STATISTICS, *available at* https://www.bls.gov/ooh/computer-and-information-technology/software-developers.htm

[17] Global Skills Initiative website: https://opportunity.linkedin.com/skills-for-in-demand-jobs

V. Conclusion

We applaud the Committee's exploration of this issue and appreciate the opportunity to offer our perspective. Our ability to prevent cybercrime depends on how quickly we allow ourselves to move. Information sharing is central to quick action, and this requires close coordination between government, experts, and the private sector. If the conditions are right, small companies like App Association members will set the pace.

Appendix: App Economy Innovators in Your Districts

Majority

Chairwoman Nydia Velázquez (NY-07)
Company: ChAPPerone

Founded by a high school physics teacher after taking 100 sixteen-year-olds on a two-week trip to Spain, ChAPPerone is a platform that allows teachers and chaperones to get important information to students without needing their personal cell phone numbers. The app includes up-to-date alerts and planning functions for before and during the trip.

Rep. Jared Golden (ME-02)
Company: Sephone Interactive Media

Sephone Interactive Media is a web and mobile software development company with a focus on marketing and online brand management solutions. Sephone helps their clients design and launch apps, websites, and digital marketing campaigns, to name a few. Their team of 10 employees has been serving clients in their Maine community and beyond since 2001 and, depending on the size of the project, will contract with developers across the country.

Rep. Jason Crow (CO-06)
Company: Peafowl Inc.

Based in Aurora and founded in 2007, Peafowl is a cross platform app development firm that takes projects from inception to completion through development, design, and testing. Peafowl has a specific focus on digital marketing and creates dynamic websites and mobile applications across several devices and disciplines for their clients. From rapper Nicki Minaj all the way to small businesses like Groundwurk, Peafowl's clients span sizes and industries.

Rep. Sharice Davids (KS-03)
Company: ActiveLogic Labs

ActiveLogic Labs is an innovative digital development agency headquartered in Kansas City with a growing presence across the United States, including an office in the Chicago area. They provide a number of services from web and desktop software development to mobile app development, all with a specific focus on user interface design and a seamless user experience.

Rep. Kweisi Mfume (MD-07), Vice-Chair
Company: Etelligens Technologies

Located in Ellicott City, Etelligens Technologies is a technology firm with a team of more than 100 employees helping businesses leverage technology to improve their customer experience. They offer mobile and web software development, user interface and experience design, as well as digital product development like software as a service (SAAS).

Rep. Dean Phillips (MN-03)
Company: Appikiko, LLC
Founded in 2015 in Excelsior, Appikiko is a mobile app developing business creating both creative and educational apps for consumers. Appikiko is a two-person team responsible for creating seven bright, interactive apps ranging from doodling and creating animated gifs and stickers, to educational K-2nd grade math practice apps.

Rep. Marie Newman (IL-03)
Company: Exemplary Marketing
Founded in 2014 in Tinley Park, Exemplary Marketing is a digital marketing agency focused on social media marketing and mobile app development for their clients. Within these two verticals, they provide an abundance of services including social media growth across Instagram, Twitter, Facebook, and LinkedIn, CRM solutions, IT management, and artificial intelligence solutions and management.

Rep. Carolyn Bourdeaux (GA-07)
Company: Digital Ignition
Founded in 2016 and located in Alpharetta, Digital Ignition is a coworking office space and start up incubator focused on fostering the tech community in North Atlanta. Similar to many coworking spaces, Digital Ignition provides not just an affordable office space, but also access to experienced mentors and investors as well as the ability to meet like-minded entrepreneurs in the area.

Rep. Troy Carter (LA-02)
Company: Jessie Health
Located in New Orleans, Jessie Health's two-person team has worked to create an online marketplace for health services, allowing patients to find the option that is right for them. Their marketplace includes health professionals, products, and services, all tailored to the patient who is able to report their symptoms before being connected to relevant options.

Rep. Judy Chu (CA-27)
Company: Virtualitics, Inc.
Founded in 2016, Virtualitics is a platform that merges artificial intelligence, big data, and virtual and augmented reality to create data visualization experiences. They make data real and actionable, allowing businesses to immerse themselves in the data through VR/AR rather than a traditional two-dimensional format.

Rep. Dwight Evans (PA-03)
Company: The Tactile Group
The Tactile Group is a Philadelphia-based full-service development agency with digital solutions ranging from web and mobile software development to strategic marketing and a strong emphasis on user experience. Their clients are in both public and private sectors, and their projects range from the Philadelphia airport's website redesign to websites for businesses in their community.

Rep. Antonio Delgado (NY-19)
Company: The Mac Works
The Mac Works, located in Bloomington, is a one-man shop providing consulting and technical assistance, primarily on Apple devices and iOS, to businesses looking for expertise on product development and launch. The Mac Works provide services including mobile app development, iOS training, cloud services, and security education and system development for Mac and iOS products.

Rep. Chrissy Houlahan (PA-06)
Company: LMG Web Design
LMG Web Design is a cutting-edge development firm located in Reading with a specialty in customizable web design and branded graphic design. Their team also assists clients with mobile application development with an emphasis on equivalent and seamless user experiences across devices and operating systems.

Rep. Andy Kim (NJ-03)
Company: Micro Integration Services
Founded in 1985, Micro Integration Services is a father and son team who transitioned from selling and maintaining hardware to an entirely software-based consulting business. MIS is focused on solving problems and helping their clients develop software for mobile and web turnkey business solutions. Although they have maintained their two-man team, Micro Integration Services works with major corporations like Kraft and the Philadelphia Eagles.

Rep. Angie Craig (MN-02)
Company: Avionte Staffing and Recruiting Software
Avionte Staffing and Recruiting Software, located in Eagan, provides solutions for payroll, attendance, billing, as well as customer relationship management, new job applications, and onboarding capabilities. Since opening their doors in 2005, they have served more than 900 customers and nearly 25,000 users across the United States and Canada.

Minority
Ranking Member Blaine Luetkemeyer (MO-03)
Company: WASHMO Media, LLC
After working as a developer for nearly a decade at companies like Mastercard and IBM, Jason Oesterly founded WASHMO Media in 2006, offering a range of services including web development and system integrations to local businesses in the area.

Rep. Roger Williams (TX-25), Vice Ranking Member
Company: App Aptitude
App Aptitude has been serving the Austin area since 2008. The team of seven provide a variety of technology related app development services for other businesses working to build out their digital presence. They create custom apps ranging from messaging and IoT to healthcare, e-commerce, and finance.

Rep. Jim Hagedorn (MN-01)
Company: AgVantage Software
AgVantage Software has been providing diverse digital accounting solutions for agribusinesses since 1976 through offerings like live accounting—which allows for inventory management—financial statements, and a variety of other features all available at the touch of a button. Located in Rochester, their software allows businesses to digitally track, analyze, and manage accounting workflows.

Rep. Pete Stauber (MN-08)
Company: Creative Arcade
Located in Duluth, Creative Arcade is a digital marketing agency that specializes in digital marketing and advertising, design and identity, web development, and inbound marketing. With five employees, Creative Arcade has a wide range of clients from West Virginia University to Fairview Range Hospital.

Rep. Dan Meuser (PA-09)
Company: LaunchDM
Located just outside of Reading, LaunchDM is a creative digital marketing studio with six employees that has been around since 1997. LaunchDM has a mix of artists and developers who help businesses with their digital branding through design, social media, web and mobile software development, branding, and search engine optimization (SEO).

Rep. Claudia Tenney (NY-22)
Company: cny apps
Located in Utica and founded by a husband and wife team, cny apps helps local businesses and restaurants connect better with their customers. They create mobile applications across both the App Store and Google Play and serve restaurants, local radio stations, and credit unions.

Rep. Andrew Garbarino (NY-02)
Company: Juiced Tech
Prior to founding Juiced Tech, the co-founders, who also happen to be brothers, had worked at large companies in IT throughout the ‘80s and ‘90s. After realizing that the industry’s growth potential, they founded Juiced Technologies in 2005 on Long Island. Juiced Technologies has now grown to 17 employees and serves primarily as a custom software development firm for businesses of all sizes providing them with apps, websites, and software to help their businesses reach the next step.

Rep. Young Kim (CA-39)
Company: Pegasus One
Based in Fullerton and with development teams across the globe, Pegasus One is a software development company whose services include artificial intelligence, custom software solutions, cloud services, and dev-ops as well as data analytics and intelligence. In addition to their development work, Pegasus One creates detailed case studies highlighting their work with each client and providing insight into the customer’s unique problem, solution, and road map to implementation so that future clients (and fellow developers) can understand their process and learn from their experiences.

Rep. Beth Van Duyne (TX-24)
Company: aTeam-Texas
Founded in 2019 in Southlake, aTeam-Texas is a full-stack software solutions firm that offers several services for their clients. They focus on Amazon Web Services, helping to find businesses experienced contract developers, and custom web and mobile software development.

Rep. Byron Donalds (FL-19)
Company: FieldEdge
Founded in 1980 and located in Fort Myers, FieldEdge is a platform that allows home service contracting organizations to digitally manage customers, work plans and execution, and important financial information. Their product includes features such as scheduling and dispatching, performance, customer management, and provides QuickBooks Integration.

Rep. Maria Salazar (FL-27)
Company: SDSol Technologies
With 68 employees today, SDSol Technologies is a software development firm located in Coral Gables with more than two decades of experience. They serve businesses and startups through the development of mobile apps, IoT products, and other custom web and software solutions. Notably, SDSol Technologies partnered with the University of Miami on a large-scale research project into the cognitive capacity of children in a range of subject domains, their technology providing the backbone of the research and enabling the university's research team to expand their subject pool.

Rep. Scott Fitzgerald (WI-05)
Company: Xorbix Technologies
Founded over 20 years ago with a location in Hartland, Xorbix Technologies is a custom software development firm helping businesses meet their customers online. They offer a number of services such as full-service custom software development, mobile app development, and general IT consulting.