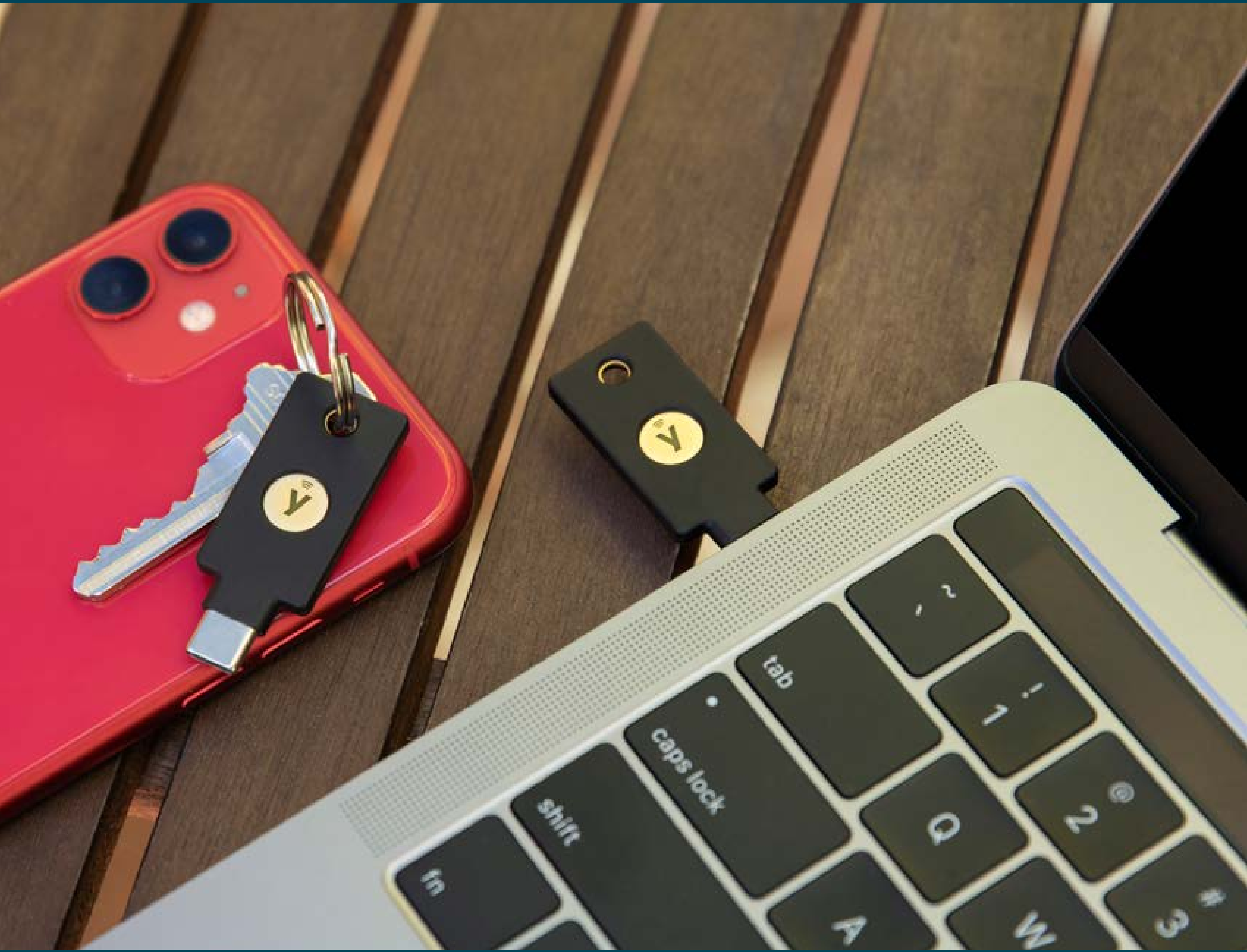
A GOVERNMENT TECHNOLOGY CASE STUDY: YUBICO



Enhancing Cybersecurity in the Public Sector:

How State and Local Governments Are Combating Account Takeovers with Hardware Security Keys

Cybersecurity has never been more important for government agencies. In 2019, governments experienced 6,843 security incidents, 346 of which involved confirmed data disclosures.[1] These incidents happen for a variety of reasons, from software installations that increase governments' attack surfaces to lost or stolen credentials.

As agencies contend with ongoing security threats, they also face evolving business needs, including modernizing their infrastructure and processes, supporting and enabling a hybrid workforce, and securing connectivity and access.

Identity and access management is critical to a well-rounded cybersecurity strategy. Passwords, which aren't effective against phishing attacks and account takeovers, offer relatively little protection. So agencies are adopting multi-factor authentication (MFA) solutions to strengthen access controls and authentication as they pursue digital transformation efforts. But some MFA tools still leave security gaps open: Mobile-based authenticators like push notifications, SMS and OTP are susceptible to malware, man-in-the-middle attacks and SIM swaps. What's more, those types of mobile solutions can frustrate users.

Remote work can increase security risks like phishing attacks and attempted account takeovers.

To combat cyberthreats such as phishing attacks and account takeovers, several state and local government agencies have turned to strong MFA using hardware security keys, one-touch authentication devices users can insert into their computers or tap against their mobile phones to securely access critical systems and applications. States and localities are already using these keys to lower risk in remote work environments, provide first responders with fast access to sensitive data, secure election infrastructure, protect confidential data on computing devices including shared workstations, provision secure access for privileged users and air-gapped networks, and deliver agile and safe citizen-facing digital services. The city of Sacramento uses this solution to make remote work more secure, while Washington state has leveraged it to protect its election infrastructure. The city of Mission Viejo, Calif., uses it to ensure business continuity in times of crisis.

As the public sector works to strengthen its security posture, adopting strong MFA using hardware security keys can help state, city and county governments increase their agility without compromising security or user experience, empowering these organizations to provide more responsive service and better meet employee and constituents' needs.

Sacramento: Building a More Secure Remote Work Infrastructure

As the remote work environment has vastly expanded due to COVID-19, government agencies have confronted exponentially more security vulnerabilities.

"Before COVID hit, people felt confident in the way they were protecting user access because everybody was working in the same location," says Cody Hussey, a solutions engineer at Yubico, which manufactures hardware authentication keys that help state and local governments improve security. "Now that some of the workforce is working from home, the mitigation needs to change."

Remote work can introduce new security risks with employees using potentially unsecured home-based WiFi networks. Even if remote employees use a virtual private network (VPN), they might still connect unauthorized personal devices or apps to this network, which jeopardizes security for the agency.

To strengthen authentication security, the city of Sacramento implemented the YubiKey, a hardware security key-based strong MFA solution from Yubico that's purpose-built to protect against phishing attacks and account takeovers. Previously, the city relied on a mobile-based voice and text OTP for authenticating employees. But that approach became a challenge once more employees had to work remotely, says Curtis Chiuu, Sacramento's principal systems engineer, as not every employee had a government-issued mobile device.

"We can't mandate our employees use their personal phones for work-related functions, so we had to come up with an alternative solution," Chiuu says.

Sacramento had previously adopted the YubiKey for a smaller number of remote employees who needed access to critical infrastructure, as well as for field workers who didn't have access to government-issued mobile devices. But with one-third of its workforce now remote, the city needed to leverage the solution more broadly to ensure secure VPN connectivity and application access for remote employees.

Chiuu says the primary advantage of key-based MFA is the ease of use.

"The biggest benefit is that you don't have to use your phone and wait for that phone call or wait for that text message with the OTP. This is such a simpler solution where I just plug it in, tap the button and I'm done."

Hardware-based MFA eliminates device-based authentication and bring your own device (BYOD)-related reimbursement expenses. Each employee also gets their own key, which also helps protect data at shared workstations. A hardware-based strong MFA solution such as the YubiKey supports multiple authentication protocols on a single security key, including OTP, SmartCard and modern FIDO U2F, FIDO2/WebAuthn authentication protocols, enabling users to securely and conveniently access different online services, bolstering security against phishing attacks and account takeovers.

All these capabilities are critical as government organizations like Sacramento shift to a hybrid work environment.

Washington State: Protecting Critical Election Infrastructure

Agencies face several election security vulnerabilities. Software- and SMS-based MFA solutions can actually increase the attack vector for election agencies, making them more susceptible to malware, phishing attacks and other security threats.

A hardware security key-based MFA solution reduces the attack surface for elections agencies because these organizations can distribute individual hardware security keys to elections staff and seasonal workers who need access to voter registration systems, e-poll books and other critical election infrastructure. Users can enter their username and password, then insert this key into the USB port on their computer and then touch a button on the key to complete the authentication process. If they are logging in via mobile, they can enroll their device via their MFA provider's mobile app. After this, they can simply tap the key against their NFC-enabled mobile device to authenticate themselves and log in.[2]

The state of Washington realized all these benefits when it adopted the YubiKey. Lori Augino, Washington's elections director, says state leaders didn't want to use a mobile-based MFA solution because they were concerned about elections staff, including seasonal workers, relying on their personal devices for government business.

Washington began using YubiKeys when it launched VoteWA, a new statewide elections management system that facilitates same-day voting and integrates election systems across the state's 39 counties. The state previously relied on allow-listing approved IP addresses, strong passwords and user permissions. By leveraging key-based MFA, Augino says, the state has added an additional layer of security. It also avoids the cost of having to purchase government-issued mobile devices for elections staff.

"I like the YubiKey as opposed to phone authentication," Augino says. "We have a lot of users within our system that don't have a state- or county-provided cell phone, and I certainly don't want them using their own personal devices for agency or office business. The YubiKey was really the easy-to-use multifactor authentication of choice for us here in Washington state to achieve the additional security needs we had."

Hardware-based security brings several benefits for elections agencies. For one, it provides greater security than mobile authenticators: A security key stops 100 percent of account takeovers, compared to a 90 percent prevention rate for on-device prompts, a 79 percent prevention rate for secondary email and a 76 percent prevention rate for SMS codes.[3] A hardware solution also operates without the need for a battery or network connectivity. And it meets NIST, FIDO and other industry-standard security and government compliance requirements.

"Modern threat tactics, techniques and practices require an improved security posture and authentication through MFA," Augino says. "It's vital to accessing these critical systems. You just can't operate without it anymore."

Mission Viejo: Enhancing Security for Digital Services

More governments are providing digital services to constituents, a crucial part of ensuring business continuity during times of crisis.

The city of Mission Viejo has embraced digital services, allowing constituents to report complaints and submit service requests to different departments, attend virtual meetings and access city records online.[4] The city even has its own mobile app — the MV Life App — that provides timely updates and allows citizens to report public safety issues.[5] These and other digital services involve collecting citizen data and reviewing it on the back end, which means employees must have secure access to systems — whether they're in the office or working remotely.

Jackie Alexander, Mission Viejo's director of information technology, says the city previously relied on complex password requirements for authentication, but decided to adopt a hardware security key-based MFA solution to strengthen its security posture.

"Despite all the user training and password restrictions in place, usernames and passwords are not enough to secure access to critical systems these days. Bad actors can use password spraying or social engineering to gain access," she says, adding that the city turned to hardware-based security to add a "second method of authentication, so even if password hacks were successful, there is a second layer of protection to get through."

As more agencies adopt software-as-a-service (SaaS) applications, hardware security key-based MFA becomes especially critical.

The city deployed hardware security key-based MFA using the YubiKey across 12 different locations, including its library and community center. All of its departments are required to use the solution to log in. Alexander says YubiKeys help the city meet high security standards, but it's also more cost effective compared to other MFA solutions. And because it doesn't require password changes as often, it provides a more frictionless experience for government employees.

As more government agencies adopt software-as-a-service (SaaS) applications and connect them to their networks to provide citizens with digital services, hardware security key-based MFA becomes especially critical. It can be paired with cloud-based single sign-on providers, giving employees streamlined, secure access to the digital applications they need to do their jobs.

"We have seen several attacks against user accounts, but they've been unsuccessful," Alexander says. "If you're not using MFA, you must find the budget to adopt this solution. It adds a much-needed layer of protection and provides protection against password exploitation."

Conclusion

In today's changing landscape, governments need a holistic cybersecurity strategy — one that doesn't wholly rely on software-based solutions to bolster security defenses. Hardware-based security is vital to protect critical government systems from both external and internal security risks.

Governments should consider incorporating hardware security key-based MFA into their security strategy as Sacramento, Mission Viejo and the state of Washington have. Their experiences demonstrate the benefits government organizations can reap by turning to physical device security.

"Without two-factor authentication, you're leaving your network and your organization vulnerable," Alexander of Mission Viejo says. "It's really important to add this layer of security. This is one among many other layers cybersecurity experts should be adopting. This is the front line. Don't start somewhere else without having this in place."

This piece was developed and written by the Government Technology *Content Studio, with information and input from Yubico.*

Endnotes:

1. *Verizon 2020 Data Breach Investigation Report*
2. *https://www.yubico.com/products/yubikey-for-mobile/*
3. *"Modernizing election security with the YubiKey" Brief*
4. *https://cityofmissionviejo.org/services-guides/how-do-i*
5. *https://apps.apple.com/us/app/mv-life/id1173015105*

Produced by:

government technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.
www.govtech.com

For:

yubico

Yubico puts an end to account takeovers for businesses and individuals. The YubiKey — the world's #1 hardware-based security key — is the most secure, easy-to-use, and affordable multi-factor authentication. The world's largest governments, technology companies, and financial institutions trust Yubico to secure their most important information, accounts, and applications. **Learn more at www.yubico.com**