yubico

U.S. state elevates security posture for its revenue department

Phishing-resistant Yubikeys provide modern approach to cybersecurity

Case study

U.S. state revenue department

Industry

- State and local government

Benefits

- Tangible time savings for setting up new systems
- Reduced support ticket incidents by 92%

Protocols

- 2FA

Products

- YubiKey 5 NFC
- YubiKey 5C NFC

Deployment info

- Full organization deployment

The Charter: Strengthen the State's finances while ensuring protection of citizen data

A state's revenue is its lifeblood. And securing revenue is critical to the mission and goals of every U.S. state. In addition to this primary mission, complying with federal and state legislation, and communicating clearly with citizens are also paramount. Doing the job well requires a careful balance of the right people, the right technology and the right procedures.

An equally important role for this anonymous state's Department of Revenue is ensuring the security of every taxpayer's personal data, and the state's IT systems, from an ever growing list of cyber security threats.

Future-proofed security strategy a critical component of successful business operations

Driving cyber security strategy is the responsibility of the state's Chief Information Security Officer (CISO), who works closely with privacy and security operations teams to moderate risk and keep state data and citizens' personal information safe.

The state's Department of Revenue has a variable workforce, which reaches its peak during the tax season. The department has a variety of employee roles that make up the team including state and local finance, tax collectors, auditors, technical services, and a compliance team.

The Department of Revenue CISO is part of the Division of Technical Services, but the job purview covers the whole organization. The CISO manages overall cyber security and also supports the physical security of the numerous systems within the state's tech stack. More specifically, he is responsible for ensuring the right technology and processes are in place to protect confidential data found in paper and electronic files related to taxes.

> "Our vision is to be the premier agency in providing innovative, accessible resources, and exceptional service built on a foundation of trust, inclusivity and creativity. We are a tax payer-focused entity. Our main role is to make sure we provide all of the tools required for businesses and individual taxpayers to make the job of paying taxes as easy as possible."

CISO's are always looking at evolving risks including sim swapping, email attacks, account takeovers, phishing, and more. Overall security strategy requires consensus with privacy and security teams to ensure there is a full picture of how to address all threats and risks. Department employees must also be trained on how to implement and leverage the strategy.

Getting ahead of the curve requires advanced security measures

The CISO had been a long-time user of YubiKeys, that delivered strong phishing-resistant multi-factor authentication (MFA), for his personal banking and other online accounts and had been looking for an opportunity to bring YubiKeys into the department to advance their overall security posture.

> "I have used YubiKeys at home for my personal accounts for more than eight years now. I use them for banking, insurance, and a lot of different websites that use MFA as well as my Windows login, where I tie it to Windows Hello and other applications that support 2FA. I have been looking to bring YubiKeys into the Department of Revenue for a while now."

He learned that YubiKeys had actually been used in this state during the 2020 election cycle to bolster security, and that city, town and county clerks were required to use YubiKeys to authenticate to the state's central election system before a voting site's ballot results could be uploaded. Given this precedence, the CISO knew the timing was right to implement them for the Department of Revenue, too.

> "Right now, the biggest risk is our individuals could be tricked into giving their information to somebody, and we'll do security training until everybody's ears are bleeding, but it still comes down to that with a piece of plastic with gold on that they have to plug into a machine. And if the hackers don't have that...they're not getting it."

The opportunity: Modernize cybersecurity by replacing RSA

The stars seemed to align for the CISO as their existing contract with security vendor RSA was due for renewal. Change was inevitable: RSA had only recently announced the end-of-life of their SecureID fobs. Even before this, some employees had been struggling to see the RSA key fob screens showing the one-time codes needed to authenticate into the system. This led to numerous daily support calls as users were being locked out due to inputting incorrect codes.

This gave the CISO an opportunity to review security across the existing tech stack and make recommendations to upgrade their security approach. The CISO consulted with their Privacy and Security team to find out what business issues needed to be solved. His goal was to mitigate and reduce risks while also lessening the workload of technical support teams, both in the implementation process as well as in the ongoing daily support requirements.

Modern MFA prevents account takeovers while increasing IT efficiency

The CISO was looking to upgrade to modern, strong MFA while also creating a whole different security process to simplify the Windows logon process and reduce the burden on support. The CISO also wanted to include Cisco inConnect VPN and their Citrix solutions. YubiKeys were the perfect fit as the MFA piece of his strategy. The Yubico team reached out to one of their partners, Green Rocket, to replace the previous proprietary OTP MFA solution with a lightweight and more flexible but still highly secure alternative.

> "Using the old encryption method and the RSA key fob required a lot of man hours. With YubiKeys and GreenRocket, the new solution for setup and encryption is down significantly to a matter of two to three minutes a laptop, and we are also now able to leverage existing tools we had already paid for, like Microsoft's BitLocker Recovery."

> We went from a five-hour setup down to a matter of 20 minutes for the actual setup and handing the machine to an individual user, by switching over to the YubiKeys and Green Radius and a different process for Opus encryption."

The existing security strategy did well with mitigating security risks and protecting the state's important data and information. However, it also was highly labor-intensive in two ways. First, it would take several technicians at least 5 hours to set up each new computer with the RSA key fobs and a full disk encryption solution. It also required rigorous training for both technicians and users to explain the numerous steps in the process.

The second challenge was the constant support calls when employees were locked out of their system. The CISO wanted to find a new streamlined, technologically-advanced approach that would put them ahead of the security curve and IRS requirements. YubiKeys are proven to reduce support incidents by 92%, saving any organization time and costs.

Privacy and Security Teams achieved 98% rollout in 3 weeks

The CISO's plan for a rollout included training for supervisors, who would then be responsible for supporting the individuals on their team. YubiKeys were sent to each supervisor who then met with the employees they were responsible for setting up. The full rollout to 98% of employees took a total of 3 weeks, while those who were remote were addressed as one-offs.

> The buy-in was rather simple for our individuals—once they saw the new solution and how it works, they saw the savings the new process would achieve, in terms of man-hours saved as well as cost savings. And we've completely eliminated issues with lock-outs. We don't have that problem any more."

Looking ahead: YubiKeys will solve more use cases over time

The CISO is currently focused on the primary use case of strengthening security across the entire department. Going forward, the CISO has a vision for how YubiKeys could be leveraged in other operations, such as helping the Department of Revenue and other state departments make the move to becoming passwordless.

> One of the selling points that we leveraged is how the YubiKeys can actually come into play in other work-related functions, such as work websites or other applications that require or could turn on multi-factor authentication to help prevent account takeovers. We can grow in our use of the YubiKeys over time as we move towards passwordless."

Passwordless authentication not only delivers a frictionless experience for users but accomplishes it while ensuring high levels of security. After all, hackers can't steal what users don't have.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
5201 Great America Pkwy, #122
Santa Clara, CA 95054, USA
844-205-6787 (toll free)
650-285-0088