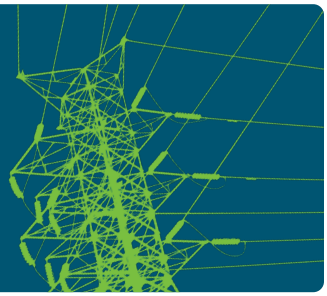
yubico

Securing critical infrastructure at an Asia-Pacific energy company



Case Study

ANONYMOUS STATE-OWNED ENERGY COMPANY

Industry

- Energy
- Critical Infrastructure

Benefits

- Secures operational technology environment
- Allows for swift login for remote employees
- No additional software required
- YubiEnterprise Subscription keeps pricing predictable and adds value

Protocols

- 2FA

Products

- YubiKey 5 NFC
- YubiKey Nano 5C

Deployment info

- All users (including third parties) who require access to OT environment
- Sysadmins, security, telecoms, SCADA users

This case study was conducted in partnership with a state-owned regional energy company, located in a major developed nation, which serves millions of customers across a territory of more than 1.5 million square kms. Their electricity distribution, retail and energy services utilize 100,000s of kms of power lines and dozens of stand-alone power stations.

Due to the sensitive nature of cybersecurity, they have requested their name be withheld.

Global energy networks are under attack

Across the world, energy systems are a target for cyber criminals. In 2021, the Colonial Pipeline was shut down for five days and a U.S. state of emergency was declared after a single leaked password resulted in a ransomware attack. Threats are not limited to ransomware: they are also a weapon of war. The Ukrainian energy grid has suffered an unprecedented number of cyberattacks in recent years, and major energy companies continue to face relentless assault.

At the Anonymous Energy Company, much of the responsibility for protecting operations from cybersecurity attacks falls to the Operational Technology (OT) Security Specialist. They sit at the border between the world of IT and OT, protecting the hardware and live equipment upon which distribution relies.

The OT Security Specialist explains the high stakes: “in our world, critical infrastructure is a high priority target for many nation states, so there will always be malicious actors looking to get in. If an attack were successful, intruders could turn off energy for millions of users, create a destabilization in the energy grid and blackout the whole state.” The consequences would be severe: “in a worst case scenario, there could be a catastrophic failure of the primary plant. Some of those things can take years to replace.”

Lives would be at risk: “staff performing work on equipment wouldn’t know if it was energized or de-energized and could get shocked. There are systems in place to protect that equipment. But if it’s under those sorts of extreme events, you don’t know exactly what’s going to happen.”

> “In our world, critical infrastructure is a high priority target for many nation states, so there will always be malicious actors looking to get in. In a worst case scenario, there could be a catastrophic failure of the primary plant. Some of those things can take years to replace.”

> For us in the OT environment, a bigger threat is APT groups: Advanced Persistent Threats, the sort of attack carried out by nation states."
>
> – OT Security Specialist at Anonymous State-Owned Energy Company

Operational technology—the critical importance of energy infrastructure

The OT Security Specialist explains that protecting the OT environment has different challenges to a typical IT environment: "we may not be that susceptible to the day to day attacks you might get in a corporate setting. In an OT environment, you don't have direct internet access, so you've cut off a lot of attack vectors. In IT, where users are dealing with email and accessing web pages, their job is a lot harder. They've got to worry about web proxies and they'll be facing new threats on a daily basis."

That doesn't mean the threat is less severe: "for us in the OT environment, a bigger threat is APT groups: Advanced Persistent Threats, the sort of attack carried out by nation states." APT attackers typically remain unnoticed in a system for a long period, often initially seeking to surveil or steal, rather than to disrupt.

The need for strong defense against phishing and other forms of account takeover

As a critical part of state infrastructure, the importance of strong cyber security practices is recognized at board level, and the organization must comply with recently-strengthened federal legislation. The OT Security Specialist received a mandate from the Chief Information Security Officer (CISO) to strengthen authentication processes for entry to the operational environment.

Users who required additional protection included sysadmins, security, telecoms, SCADA users and anybody who performed a function within, or supported, the Operational Technology environment. Users are distributed throughout the state, across different offices, worksites and remote locations.

Employees and third-party contractors access the operational environment via the corporate WAN using F5 VPNs, which function in tandem with Microsoft Active Directory. Previously, access was possible with just a username and password. As global cybersecurity risks rise, multi-factor authentication (MFA) becomes an essential measure to protect organizations. Adding a second phishing-resistant authentication factor was seen as a necessary, proactive step to mitigate against growing threats.

Any MFA is better than a password, but not all MFA is built equal

During the procurement process, The Anonymous Energy Company had to balance multiple requirements. It was important that the product would also integrate easily with existing infrastructure, without requiring additional software. This ruled out one possible solution—smartcards—which require specific drivers and smartcard readers to function.

The OT Security Specialist was also keen to find a solution that was user-friendly, "we did have the user in mind, because you can get a lot of backlash if you deliver something that people don't like. If we required TOTPs [Time-Based One-Time Passwords] for all accounts, users could have six different TOTPs to select from their phone and type in."

The foremost consideration was security. SMS authentication can be hacked, and is not suitable for remote locations with poor mobile reception. The OTP Security Specialist also had doubts about one-time passwords: "to be honest, I see it as less secure. If you know the initial key that was used to set up the TOTP [time-based one time password], you can pretty much get in. And if you're able to trigger an authentication request, somebody only has to click approve, and employees might just approve it automatically since it has come up on their phone."

Yubico—securing the OT environment gateway

The limitations of alternatives, combined with the proven security track record, made physical security keys the obvious solution. The OT Security Specialist was most attracted by how YubiKeys balanced security and usability: "if you've got to physically touch the button, you know a user is physically there using it. We could set up one YubiKey as MFA for all a user's accounts, so they don't need six different TOTPs."

YubiEnterprise Subscription

Learn more about YubiEnterprise Subscription.

At the end of the day, it was a simple choice: “we just kept coming back to the YubiKey. We dug into it a bit deeper and found we could implement YubiKeys quite easily using our existing infrastructure. After that, we were quickly able to do a proof of concept and move forward.”

YubiEnterprise Subscription offered high-level security with low cost-to-entry

The Anonymous Energy Company chose an initial purchase of 500 YubiKeys through YubiEnterprise Subscription to secure all users who access the operational environment. The models chosen vary between job roles, with YubiKey 5 Nanos, which are intended to stay in your PC, suiting those who remain in the central office and YubiKey 5C NFCs selected for employees who more often require remote access.

YubiEnterprise Subscription helped maximize value by offering a simplified and flexible way to adopt strong phishing-resistant MFA. The predictable cost suited their buying model, with the added benefit that 25% of purchased keys can be upgraded or replaced over the three-year subscription period. The multi-year terms allowed low cost to entry and faster time to value, as well as the security of knowing that lost or stolen keys would be replaced and new keys added to account for new hires and employee churn. Prioritized access to technical support and automatic upgrades to new models all meant that the highest possible level of protection would always be guaranteed.

A swift deployment process

According to the OT Security Specialist, deployment has been successful: “we haven’t had any technical issues. We were able to find a guide on the Yubico website which was very useful for doing proof of concept, though the end result looks a little different. We’ve got something that’s going to work and should support us going into the future, without having to spend any extra time or money on additional software, which was a big benefit.

“We’ve got a more secure environment. The actual logins are fairly quick and users found it an easy process to start using them. As long as they had a spare USB port on their computer, it was easy.” Users have been encouraged to also use YubiKeys for their private accounts.

> “My personal opinion is that they’re more convenient to use than a token off your phone, especially when your YubiKey is next to you. I don’t like having to grab my phone and look for an app to get a token out of it or unlock it to approve a request. It’s a lot quicker to just hit a button on the USB stick.”
>
> – OT Security Specialist at Anonymous State-Owned Energy Company

A passwordless future is possible

The immediate benefits mean further use cases will be explored: “Previously it was just username and password but now we’ve got that additional layer of defense with the YubiKey. At the moment that’s the primary use case but we are looking to leverage more features in future.”

“We’re interested in the smartcard functionality, too. We may even look at some sort of password-less integration, so once people are inside the environment, they don’t have to use their password as much—they can use the YubiKey. It’s not a short-term goal, but our users would love to not have to put a password in!”

As the case of the Anonymous Energy Company shows, it’s clear that usability and cost can never be ignored, no matter the security risk. Relying on ever-changing passwords or unreliable mobile authentication doesn’t just irritate employees, it provides opportunities to cyber criminals. As cybersecurity risks rise, it’s essential that companies, and governments, do everything in their power to protect the critical infrastructure and energy distribution upon which society relies.

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