yubico

Maximizing security across Pharma's digital transformation with phishing-resistant MFA

Secure data, technology, and people against modern cyberthreats

Introduction

The COVID-19 pandemic has accelerated the existing digital transformation across the pharmaceutical industry with the aim to accelerate time-to-market while reducing overall costs. However, the irony of such rapid paced innovation is that it can create a gap when the rate of technology adoption outpaces its own security organizations process to implement safeguards for identity and authentication, leaving IP and critical business applications vulnerable to attack.[1]

Pharmaceutical companies are often the target of state-sponsored cyber espionage attacks. For instance, in 2020 the former head of the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency warned that North Korea, Russia, China, and Iran all attempted to infiltrate companies working on COVID-19 vaccines in countries around the world.[2]

In addition to state-sponsored cyber espionage attacks, pharmaceutical companies are also at risk of more common cyber threats such as brute force, phishing, and exploitation of vulnerable web applications. In these types of attacks, hackers frequently use phishing or spear phishing tactics that contact targets through fake or compromised email accounts, to dupe the target into revealing valuable information which may then be used to launch additional raids upon the company.

According to BlackCloak, 68% of pharmaceutical executives' emails have been exposed in a data breach since 2010.[3] Of those exposed, 57% of the hacked passwords have been viewable on the dark web.

Regardless of the origin or institution behind the attack, today's well devised devious plans seek to disrupt functional areas of the business who develop and manage the greatest asset of any pharmaceutical organization—intellectual property.

These organizations and their partners—Clinical Research Organizations (CROs), Active Pharmaceutical Ingredient (API) manufacturers, Contract Development and Manufacturing Organizations (CDMOs), Cloud platforms & Software-as-a-Service (SaaS) providers, are not surprisingly also the same ones implementing modern technology to speed time to market and reduce costs via enhanced data collection, analysis and communication across a distributed global network. Hence, it is no surprise to see the volume of attacks increasingly focused here; one small opening can offer access to critical systems and data.

Insider threats are also a credible and ongoing risk. For instance, foreign adversaries often attempt to exfiltrate sensitive data by bribing an inside employee, or by planting a spy within the company. In addition, disgruntled employees, such as those facing layoffs, may also seek retribution and therefore represent an additional insider threat.[4]

The 2021 ransomware risk pulse: pharmaceutical manufacturing[5]

- Pharmaceutical companies' annual cyber attack risk averages $31.1 million
- Almost half of all pharmaceutical companies have more than 1,000 leaked employee credentials exposed on the deep web
- Nearly 10% of pharmaceutical manufacturers are highly susceptible to a ransomware attack
- Data management vendors pose the most significant annual financial risk ($6.2 million) to pharmaceutical manufacturers in the supply chain

Economic consequences of cyber attacks

Pharma and biotech companies face the greatest risk

According to the 2021 Cost of a Data Breach Report, the average cost of a breach in the pharmaceutical industry was $5.04 million, just behind healthcare and financial services industries.[6]

The already high costs of data breaches are continuing to rise, and some can result in catastrophic losses, such as the $1.3 billion Merck breach in 2018.[7] This attack disabled more than 30,000 laptop and desktop computers and more than 7,500 servers. Departments across the entire organization, including sales, manufacturing, and research units, were all impacted. Some employees reported that they lost as much as 15 years of research and data. Ultimately, the attack brought a halt to Merck's production of the leading vaccine against human papillomavirus.[8]

The consequences of lost high value IP through the asset development process via CROs and biotech companies, then through FDA approval, and subsequent commercialization technology transfers to CDMOs cannot be underestimated. With the average cost of bringing a new drug to market estimated at more than $1 billion (USD), losing first-to-market advantage can be devastating to a company's revenue and market share.[9] Cyber espionage can occur throughout the product lifecycle, whether it's the discovery phase, FDA approval phase, or the commercialization phase, making it imperative that all digital data related to Active Pharmaceutical Ingredients (APIs), as well as commercial product management procedures, are tightly secured.

Cybersecurity is more important than ever

Although the pandemic created a heightened sense of urgency for drug and vaccine development, speed is always a critical factor in the pharmaceutical industry. Not only is it essential to make effective, life-saving drugs and vaccines available as quickly as possible, it's also key to staying competitive and maximizing shareholder value.

However, staying competitive depends on more than being first—it also depends on keeping valuable IP and critical data secure across the entire product lifecycle. As a result, pharmaceutical companies face unprecedented demand for powerful and effective cybersecurity solutions to minimize their exposure to cyber espionage and other threats. To protect their organizations, security leaders first need to understand the technological challenges and vulnerabilities both within their companies and across the supply chain, including CDMOs and other third party partners and vendors.

This paper will focus on best practices for pharmaceutical organizations but applies to all organizations across the product lifecycle, including research labs, biotech companies, trial partners and clients, and CDMOs.

Challenges in securing the pharmaceutical landscape

The pharmaceutical industry shares many of the same challenges global enterprises face. Although agility and innovation are essential to remaining competitive, embracing "digital transformation" across every level of the technology infrastructure is simply not possible yet. This is because securing complex, global infrastructures is hindered by multiple challenges.

1. Complex, hybrid infrastructures are hard to integrate

Like most large companies, pharmaceutical firms constantly struggle to integrate, manage, and secure a complex mix of legacy and modern systems. For instance, not all organizations have fully migrated to the cloud, and many still maintain disparate data and applications in siloed data centers. Although concerns about security are partly why pharmaceutical firms have been reluctant to move everything to the cloud, that trend is quickly changing given the widespread demand for remote access to data and applications.[10] Today, in addition to legacy systems, cloud apps, SaaS, IoT, and IoT device integrations comprise a large part of the technology complexity across pharmaceutical companies.

2. Corporate growth can destabilize cybersecurity efforts

For large organizations, Research and Development (R&D) acquisition is becoming the norm. Integration challenges further exacerbate security issues because it's simply not possible to execute a uniform cybersecurity approach across all of these disparate systems and point products. What's more, to save time and money organizations may attempt to retrofit legacy systems rather than deploy new technology—a migration process that can disrupt business continuity.

3. Digitized data flows everywhere

Pharmaceutical IP is now all digital, and can be uploaded, stored, and shared on virtually any device. These digital assets often include highly proprietary formulas for molecules and APIs, as well as other strictly confidential data. Cybercriminal organizations target pharmaceutical companies precisely because this data is incredibly valuable—and vulnerable—and can be easily sold on the dark web or ransomed back to companies for outlandish payments.

4. Strict government regulations add complexity

Pharmaceutical companies must adhere to a number of government regulations to ensure the safety and efficacy of their products. They also have to ensure patient privacy and data accuracy by meeting compliance requirements such as the General Data Protection Regulation (GDPR) in Europe, and HIPAA, 21 CFR Part 11 (Code of Federal Regulations Title 21) by the Federal Drug Administration (FDA), and Drug Supply Chain Security Act (DSCSA) in the U.S. All of this adds further complexity to how pharma companies secure and manage access to their data.

5. Shortage of cybersecurity skills limits access to resources

It's no secret that the scarcity of cybersecurity resources is compounding the security challenges pharmaceutical companies already face.[11] With fewer resources to meet IT security needs, existing staff struggle to manage growing workloads. On top of that, open jobs are often filled with junior personnel who lack adequate experience and training for various security responsibilities. As a result, IT organizations may not be using their current security technologies to full potential. Doing so could help automate many routine tasks and free up senior IT professionals for more strategic initiatives.

6. Reliance on third party vendors can increase risks

Reliance on outsourced partners like CROs and CDMOs require IP handoffs that can result in major vulnerabilities. If the weak links in the chain aren't addressed and strengthened, pharmaceutical organizations can face costly consequences and delays in time to market.

Critical stages most vulnerable to cyber espionage

Credential theft from phishing is one of the main cyberattacks targeting pharmaceutical companies. Hackers may break into an inadequately secured database or use phishing and spear phishing techniques to steal employee credentials. This is why username and password single-factor authentication is not an adequate form of security. Additionally, many employees reuse passwords across applications (in both business and personal accounts), leaving organizations at risk of attack even if an employee credential is compromised outside of the corporate network.

Below are critical phases through the product lifecycle that are most vulnerable to cyber espionage attacks.

Discovery	Clinical Development **Phase 1**	Clinical Development **Phase 2**	Clinical Development **Phase 3**	**FDA**	**Commercialization/ Scale out**
• Engineering of drug and vaccine molecules and compounds • Lots of third parties involved during formulation	• Many third parties involved in clinical trials	• Licensing and acquisition • Major process handoffs and scale up including during technology transfers	• Licensing and acquisition • Major process handoffs and scale up including during technology transfers	• Maximum IP value, maximum IP exposure (new clinical trials, expanded teams)	• Proprietary manufacturing process • Significant expansion of supply chain (CDMOs)

Close the digital threat gap by protecting your users with phishing-resistant authentication

The IMB Cyber Security Intelligence Index Report states that 95% of all breaches are caused by human error.[12] Closing the threat gap not just against current cyber threats but also future ones starts with the right authentication solution for your users. Legacy authentication such as usernames and passwords, and mobile-based authentications increase the probability of human error, and in turn, the risk of being breached. By protecting your users with strong phishing-resistant authentication, and ultimately eliminating passwords altogether, the integrity of pharmaceutical IP is ensured.

> **Human error was a major contributing cause in 95% of all breaches.**
>
> —IBM Cyber Security Intelligence Index Report

Not all MFA is created equal

Early generations of two-factor and multi-factor authentication relied on usernames and passwords along with mobile-based authentication such as one-time passwords (OTP), SMS codes, and push notifications. However, in addition to being easily guessed or stolen, usernames and passwords are cumbersome and expensive to manage. For instance, Forrester estimates that help desk calls for password resets can cost a company an average of $35 per incident.[13]

On the other hand, mobile-based authentication such as push notifications, OTP, and SMS codes are highly vulnerable to malware, SIM swapping, and man-in-the-middle (MiTM) attacks. They also offer a poor user experience because users must wait to receive the code and then enter it on their device to authenticate. And, in mobile-restricted or low connectivity areas, mobile authenticators don't work at all.

The YubiKey: how security and transformation unite

Modern strong two-factor, multi-factor, and passwordless authentication

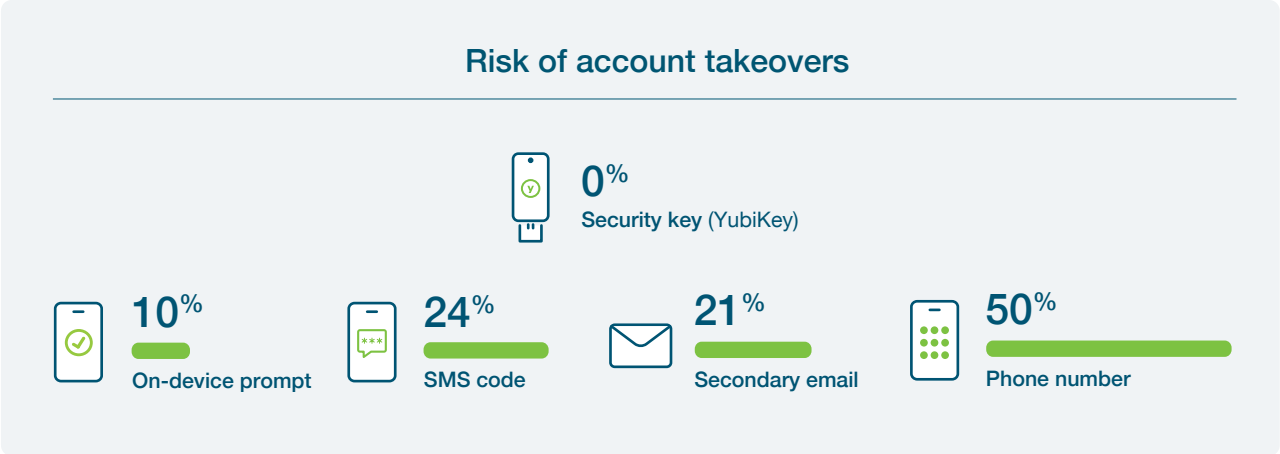
Zero trust security framework requires strong authentication at its core—and Yubico delivers it with the YubiKey. The YubiKey is a hardware security key that provides strong two-factor, multi-factor, and passwordless authentication to stop successful phishing attacks and account takeovers. To authenticate, users simply tap or touch the YubiKey. And, because the YubiKey offers USB, NFC, and Lightning form factors, it enables authentication to any system or device, including mobile and tablets.

The YubiKey provides an ideal solution for protecting pharmaceutical IP across a highly complex product lifecycle by offering:

1. Simple, strong, and portable authentication that stops phishing

Strong authentication provided by the YubiKey offers far superior protection compared to username/password credentials and mobile-based authenticators.

The YubiKey is FIPS 140-2 validated, Overall Level 1 (Certificate #3907) and Level 2 (Certificate #3914), Physical Security Level 3, and is the only solution proven to eliminate account takeovers in independent research, enabling pharmaceutical companies to move toward a future that is far less vulnerable to phishing attacks and credential theft.



Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

The YubiKey doesn't just provide strong authentication—it is also highly portable and easy to use. A single security key works across multiple devices such as desktops, laptops, mobile, tablets, and notebooks without requiring a battery or internet connection. Users can authenticate with a simple touch or tap, which provides the easiest experience possible. This is especially critical in labs and clean rooms, where mobile phones are not allowed and employees must follow strict disinfection procedures. YubiKeys are also water-resistant, crush-resistant, and easy to disinfect. By simply tapping a YubiKey, users get secure and instant access, all while upholding pharmaceutical security, safety, and productivity.

2. Highly scalable authentication with a high-security ROI

A single YubiKey supports multiple authentication protocols—smart card and FIDO2 strong authentication protocols, as well as OTP and OpenPGP. This means that a single key can be used for authentication across both legacy and modern applications and infrastructures.

The YubiKey for smart card authentication offers pharmaceutical organizations strong authentication with simple usability and high scalability. Unlike traditional smart cards, YubiKey for smart card authentication doesn't require peripheral readers, which can be expensive to deploy and scale across a global infrastructure that includes third-party vendors, suppliers, and distributors. Instead, users simply plug the YubiKey into their device and tap or touch to authenticate, along with a PIN.

Users also have the ability to store their SAFE-BioPharma certified identity credentials or other PIV-compatible certificate-based signing schema on the YubiKey to guarantee high-assurance identity trust for digital signing of cyber transactions.

3. Reduced demand on essential and costly IT resources

The YubiKey addresses the shortage of critical cyber skills by dramatically reducing IT time and costs related to password resets. Consider that, without the YubiKey, the average enterprise can spend up to $1 million every year on staffing and infrastructure expenses just to handle password resets.[14]

YubiKeys virtually eliminate the expense of password management by enabling self-service password resets without requiring users to wait for a help desk response, thus lowering costs related to downtime and lost productivity. This is especially important for applications and environments that users access infrequently—and where they are therefore more likely to forget their passwords.

Case in point: After deploying YubiKeys, Google realized a 92% reduction in password management incidents, which saved the company thousands of hours per year in support costs.[14]

4. Open, comprehensive, standards-based authentication that's easy to deploy and integrates with leading third-party platforms

YubiKeys can be used to enable MFA for identity access management (IAM) systems and identity providers (IdPs) such as Microsoft Azure Active Directory, Okta Workforce Identity, PingID, and many more. A single YubiKey supports multiple authentication protocols including FIDO2, FIDO U2F, OTP, SmartCard (PIV), and OpenPGP, ensuring strong authentication across both legacy and modern applications.

YubiKey authentication also leverages open-source FIDO authentication standards that use public key cryptography developed through the FIDO Alliance. In addition to being far more secure than passwords and SMS OTPs, authentication solutions built on FIDO standards are easier to use, deploy, and manage. This is because FIDO authentication replaces password-only logins with secure, fast, one-tap or one-touch login experiences across websites and apps.

Yubico also makes it easy to procure strong authentication and get it directly into the hands of employees. With YubiEnterprise Services, enterprises can easily procure and distribute YubiKey authentication solutions for employees at scale. A YubiEnterprise Subscription greatly simplifies how businesses procure, upgrade, and support YubiKeys. Plus, with YubiEnterprise Delivery, keys can be delivered to employees wherever they work—at home or in the office—across the globe.

Bridge to a passwordless future

We know that passwords and mobile-based authenticators can't provide the robust yet simple security pharmaceutical companies need to defend against cyber espionage. However, the journey to passwordless isn't a matter of flipping a switch, so it won't happen overnight. It requires a Zero-Trust security foundation built upon strong authentication that eliminates security gaps on a global scale.

As a fundamental part of the digital cleanroom, YubiKeys provide an ideal solution to help pharmaceutical firms move toward a passwordless future through strong MFA and passwordless authentication that can be quickly and easily deployed anywhere and used to access any device. With the YubiKey, organizations can implement FIDO2 passwordless authentication or smart card passwordless authentication or even a hybrid strategy, depending on the existing infrastructure and use cases.

The evolutionary path to strong, modern authentication is exactly what the YubiKey was designed for, because it delivers the simple security pharmaceutical organizations need along every step of their journey to becoming a passwordless enterprise and a digital cleanroom.

Economic benefits of the YubiKey

Outside of technological and security benefits, there are also economic benefits of the YubiKey for modern strong authentication. This section showcases an example authentication problem and suggested calculations that pharmaceutical organizations can use to generate estimated expected economic benefits of deploying YubiKeys for strong two-factor, multi-factor, or passwordless authentication.

SITUATION

As an example, let's consider Pharmaceutical Company X that has 100 employees who work on the commercial product management process. Company X has growing concerns over repeated cyber attacks, as well as reports of poor user authentication experience that challenges worker productivity, drives up support costs, which may also be tied to longer time to market.

The company's current two-factor authentication process includes a username, password, and a TOTP token code, which simply isn't feasible for employees who need to authenticate multiple times per day. In addition, employees often lose or misplace their TOTP tokens, which creates additional downtime and security risks. Furthermore, the time it takes TOTP codes to fully update prevents users from completing the login process in a single attempt. In fact, in some cases users needed up to three attempts to authenticate.

END STATE: MIGRATION TO PASSWORDLESS AUTHENTICATION

The office of the CISO is now exploring a means to migrate to a passwordless authentication environment for two primary reasons. The first is to reduce exposure to outside threats that are typically well funded from known nation states, and designed to disrupt R&D efforts and pilfer critical intellectual property. The second reason is to improve the employee user experience in order to drive efficiency and productivity.

With the average cost of 'drug to market' being upward of $1B, Company X's strategic priority is to incorporate a FIDO2-based passwordless strategy that would add significant incremental value to the organization.

ROI FORECAST & GOALS

It is predicted that a migration to Yubico's wearable YubiKeys with FIDO2 authentication protocol and NFC capability will address all of the above stated challenges.

The goal is to calculate reasonable, achievable, and believable hard dollar return on investment (ROI) that has been in proof of concept and positively reflects a commitment and investment in a long-term authentication strategy. For the purpose of this exercise, this means a standard, enterprise-wide method of verifying user identities without the use of a password or any other memorized secret.

GOALS

1. **Improved authentication experience:** Within the commercial product management process exist several recurring data access and entry steps. The YubiKey's ease of use drives expectations that the average authentication/login time for users will dramatically decrease per user overtime.
2. **Redirected employee productivity gain:** With the Yubikey's simple tap/touch login, Company X anticipates significant gains in lab worker efficiency, compressing the time between data updates, hence reducing the end-to-end time of completing lab-based-tasks.
3. **Help desk cost reduction:** A majority of the calls to the IT help desk at Company X are related to password resets. IT management would like to reduce the costs and time spent on password reset calls by moving toward a self-service model and eventually a passwordless environment.
4. **Threat remediation savings:** Given the fact that the highest volume of credential theft is from successful phishing attacks, Company X anticipates a significant reduction in costs related to cyber threat mitigation and remediation efforts including threat analysis, thus decreasing related security operations center (SOC) analyst Full Time Employee (FTE) cost, and importantly reducing risks to brand exposure.

ROI EXECUTIVE SUMMARY

After a comprehensive review of the above use cases, Company X has determined to move forward with YubiKeys for employees that are part of the commercial product management team. Company X will arrive at a homogeneous FIDO2-based passwordless strategy by the end of 2024, and in that time the rollout of YubiKeys would return more than ~$2M, if YubiKeys are implemented for the commercial product management team as listed in this example, including, but not limited to, significant reduction in authentication time, redirection of employee time to other priorities (other than authentication issues/inefficiencies), reduced support calls to IT help desk, and in a similar manner, reduced phishing threats to the end users, resulting in fewer cases to resolve by the security operations center. The annual ~$2M return does not include the reallocation for FTE time to higher priority deliverables such as research, development, testing, etc.

Furthermore, as this particular study was originated and managed by the office of the CISO, it is focused on the effect of technology (authentication and integration into the current application architecture), and was not focused on operational process, time to patent, time to market, or even fraudulent risk. Hence, it is believed that the resulting economic data, as shown below, is a conservative proposed estimate.

ROI CALCULATIONS

A roll-up of each estimated economic impact calculated against individual use case goals is shown in Table 1.

Table 1: ROI executive summary

USE CASE: COMMERCIAL PRODUCT MANAGEMENT | AUTHENTICATION				
Details	**Number of Employees**	**Current TOTP Cost**	**Cost with YubiKey**	**Est. Annual Return***
Authentication experience	100	$1,120,000.00	$ 560,000.00	$ 560,000.00
Redirected employee productivity gain	100	$ 22,400.00	$ 9,600.00	$ 12,800.00
Help desk costs	100	$1,400,000.00	$ 420,000.00	$ 980,000.00
Threat remediation costs	12	$1,036,800.00	$ 342,144.00	$ 694,656.00
Total Estimated Annual Return				**$2,247,456.00**
Total Estimated Annual YubiKey Costs				**$ 45,000.00**
TOTAL ESTIMATED ECONOMIC IMPACT (SAVINGS) **Total Annual Return - Total Annual YubiKey Costs**				**$2,202,456.00**

*Estimated Annual Return = Current TOTP cost - Cost with YubiKey

Table 2 shows inputs and calculations of migrating from TOTP authentication to FIDO2-based passwordless with the YubiKey, specifically the comparison of current required time for the TOTP process and its comparison to the upgraded YubiKey authentication experience.

Table 2: Authentication experience inputs & calculations

COMPANY X INPUTS			
Number of employees in use case		100	Input value
Mean hourly FTE employee rate		50	Input value
Mean minute FTE employee rate		0.83	Input value
Average days in commerical product management cycle		120	Input value
Number of commercial product management cycles per year		2	Input value
AUTHENTICATION COSTS	**CURRENT TOTP COSTS**	**COST WITH YUBIKEY**	
Number of authentication attempts per day *(include deglove, sanitation, reglove)*	8	8	Input value
Average minutes per authentication	7	3.5	Input value
Total avg daily authentication minutes invested	56	28	#attempts X avg min per attempt
Cost per authentication/employee/day	$ 46.67	$ 23.33	minute rate of employee X total daily avg time to auth
Total daily cost to authenticate (per total employees in use case)	$ 4,666.67	$ 2,333.33	cost per auth/emp/day X #employees
Total cost per drug commercial product management cycle	$ 560,000.00	$ 280,000.00	total cost per employee per cycle X #employees
Total annual authentication experience costs	**$1,120,000.00**	**$ 560,000.00**	**total cost per employee per cycle X #employees X #cycles**
ANNUAL ESTIMATED YUBIKEY COSTS			
Annual cost of licensing YubiKeys for 100 employees considering Perpetual license, 2 keys per employee		$ 10,000.00	YubiKey License
Annual support services cost considering Silver Tier Support Services		$ 35,000.00	Yubico Silver Tier Support Costs
Total Annual Estimated YubiKey Costs		**$ 45,000.00**	**YubiKey annual licensing + support costs**

Organizations can use the formulae below to calculate the estimated cost savings for use case goals: Redirected employee productivity gain, help desk cost reduction, and threat remediation savings.

Help desk cost reduction:

Inputs and calculations of migrating from TOTP authentication to FIDO2-based passwordless with the YubiKey, and the elimination of "password reset" tickets, reduction in new hire education, and ongoing support of all users pertinent to the improved authentication experience. See appendix for input data values used.

Total cost = Fully loaded help desk worker FTE hourly cost X number of help desk agents addressing password/ authentication tickets X time per agent per ticket X number of tickets per agent

Threat remediation costs:

Inputs and calculations of migrating from TOTP authentication to FIDO2-based passwordless with the YubiKey, and its impact on cyber threats and threat remediation due to non-shared-secret, asynchronous methods that stops credential phishing, malware, and MiTM driven cyber attacks. See appendix for input data values used.

Total FTE cost per remediation analysis/fix = Fully loaded security analyst FTE hourly cost X number of analysts involved in remediation efforts of suspected crediatail theft reported or detected X number of hours invested per investigation

Redirected employee productivity gain:

Inputs and calculations of migrating from TOTP authentication to FIDO2-based passwordless with the YubiKey, and the outcome of a greatly improved user experience which returns time back per authentication/login attempt, multiple times per day across the comprehensive commercial product management life cycle.

Total FTE cost per credential input/authentication = Fully loaded lab worker FTE hourly cost X number of employees involved in commercial product management process with use case requirements X average credential submissions/ authentications per development process X avg time per attempt (include clean room sanitization steps if required)

The difference between current TOTP and estimated YubiKey costs will represent the time which each lab worker may reinvest into the commercial product management process, improving the FTE cost per drug release. Further, time gained per FTE may be reallocated to other prioritized aspects of the process, hence potentially reducing time to market. See appendix for input data values and calculations.

Appendix

Number of help desk employees (in use case)	100	Input data
Help desk employee mean hourly FTE	50	Input data
Help desk employee mean minute FTE	0.83	Input data
Help desk employee work days/year	200	Input data
Number of password reset requests per day to help desk	12	Input data
Avg minutes required per password reset request	7	Input data
Total minutes/day required for password reset requests	84	#requests X avg min per
Total hours/day required for password reset requests	1.40	#daily mins / 60
Number of SOC analyst employees (in use case)	12	Input data
SOC analyst mean hourly FTE of analyst in threat remediation	90	Input data
SOC analyst mean minute FTE of analyst in threat remediation	1.50	Input data
Work days/year of SOC analyst in threat remediation	200	Input data
Number of unresolved phishing attempts per day	6	Input data
Average minutes required per analysis and remediation	48	Input data
Total Minutes/Day per SOC analyst	288	#daily unresolved X avg min per analysis
Total Hours Per Day/SOC analyst	4.80	total minutes / 60

	CURRENT TOTP	WITH YUBIKEY	
Total Authentication Minutes per Cycle	6,720.00	2,880	#minutes per day X total days per cycle
Hours Per Cycle/Employee	112.00	40	total avg minutes per day/60 (minutes)
Total Avg Daily Authentication Minutes Invested	56	24	#attempts X avg min per attempt
Hours per Year/Employee	224	96	total hours per cycle X number cycles
Total Hours/Year	22,400	9,600	total auth hours per year X number of employees

Sources

[1] https://www.wsj.com/articles/north-korean-hackers-are-said-to-have-targeted-companies-working-on-covid-19-vaccines-11606895026
[2] https://www.cnbc.com/2020/12/06/former-top-cybersecurity-chief-says-russia-china-iran-and-north-korea-are-trying-to-steal-coronoavir.html
[3] https://blackcloak.io/the-path-of-least-resistance-%E2%80%92-pharmaceutical-executive-credentials-line-the-dark-web-as-criminals-look-to-exploit-crisis/
[4] https://www.boozallen.com/content/dam/boozallen_site/ccg/pdf/thought_p/5-facts-about-cyber-and-pharma.pdf
[5] https://blackkite.com/wp-content/uploads/2021/05/The-2021-Ransomware-Risk-Pulse-_-Pharmaceutical-Manufacturing.pdf
[6] https://www.ibm.com/account/reg/us-en/signup?formid=urx-50915
[7] https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war
[8] https://blackkite.com/wp-content/uploads/2021/05/The-2021-Ransomware-Risk-Pulse-_-Pharmaceutical-Manufacturing.pdf
[9] https://www.healthcare-economist.com/2021/04/15/average-cost-to-bring-a-drug-to-market-is-over-1-billion/
[10] https://www.pharmexec.com/view/more-cloud-on-the-horizon-for-pharma
[11] https://www.csoonline.com/article/3571734/the-cybersecurity-skills-shortage-is-getting-worse.html
[12] https://www.forrester.com/report/Making+The+Business+Case+For+Identity+And+Access+Management/-/E-RES80481
[13] https://www.forrester.com/report/Best+Practices+Selecting+Deploying+And+Managing+Enterprise+Password+Managers/-/E-RES139333
[14] https://www.yubico.com/resources/reference-customers/google/

yubico

About Yubico

As the inventor of the YubiKey, Yubico makes secure login easy and available for everyone. The company has been a leader in setting global standards for secure access to computers, mobile devices, and more. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F), and open authentication standards.

YubiKeys are the gold standard for phishing-resistant multi-factor authentication (MFA), enabling a single device to work across hundreds of consumer and enterprise applications and services.

Yubico is privately held, with a presence around the globe. For more information, please visit: www.yubico.com.