Goldman Sachs | TRANSACTION BANKING

Building a Better Platform for Privileges and Authentication

Introduction

As digital technology deepens its presence in corporations, cybercrime continues its proliferation on the risk landscape.

In a survey conducted at the 2019 annual conference for the Association for Financial Professionals (AFP), 88% of corporate practitioners reported that their organizations had been victim to actual or attempted cyberattacks in the prior 18 months.[1] The vast majority (82%) of respondents at last year's World Economic Forum said they expected cyberattacks involving financial and data theft to increase—and 80% predict disruption to their business operations.

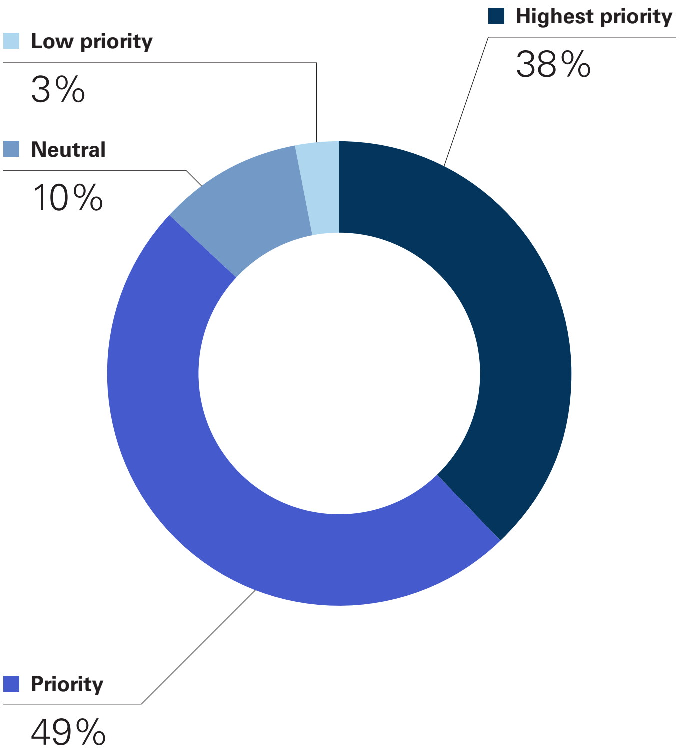
For corporate treasurers, cybercrime is an acute issue: more than half of the treasury professionals surveyed by the AFP (55%) said cyber-security risk is currently their top challenge, and it's expected to persist as their most complex risk to manage three years from now.[2]

There's a wide range on how high the stakes are, though even the low end is far from insignificant. On the high end, Cybersecurity Ventures says damages from cybercrime will hit $6 trillion annually by 2021, double what it was five years earlier.[3]

When Goldman Sachs set out to establish a transaction banking platform, we analyzed the numerous tools and methodologies companies have employed to re-think and mitigate cyber-related risks. Some commonly used tools have proved helpful; others not so much. And, as a result many companies are mired with legacy infrastructure and mindsets—firewall rules, outdated credentials and hard-to-update databases and servers. Further, we recognized that many transaction banking platforms today have evolved

Top of Mind

Level of priority treasury and finance functions place on cybersecurity, relative to other challenges.



Source: *2019 AFP® CYBERRISK SURVEY*, Association for Financial Professionals.

into a mishmash of various regional operations, a Frankenstein-like system of separate platforms and/or upgrades patched together sporadically over time. As a result, these systems are expensive to maintain and cumbersome to use—and often are outmatched by today's cyber threats, and fall short of providing the trust being placed upon them.

The result of our analysis was to create an alternative: a modern, flexible, cloud-native transaction banking system with state-of-the-art approaches for anticipating, thwarting and responding to critical security issues. One of the advantages that we found in setting up Goldman Sachs' platform from scratch is that we could survey the landscape with fresh eyes—determining which issues are of highest concern to platform users and identifying the best solutions available to meet those challenges.

When we spoke to hundreds of treasury executives to glean insight into their most pressing concerns and their biggest cyber-security challenges, some common refrains emerged. Among them, privileges and authentication proved to be seemingly intractable security issues. Ensuring that the right people within an organization have the proper authority to conduct specific transactions, and that those individuals also have the ability to swiftly and securely access their company's platform, remains a time-consuming challenge for many corporate treasurers. For example, one US-based corporate treasurer said he spends half of his time sifting through privileges and managing entitlements—keeping him away from other facets of his job. Meanwhile, the importance of authentication is manifest; we're entrenched in an era in which breaches are not uncommon and when even a single lapse in access and one rogue transaction can mean millions of dollars of lost money.

Here's how Goldman Sachs' transaction banking platform is approaching these two pressure points within treasury departments. ■

One of the advantages that we found in setting up Goldman Sachs' platform from scratch is that we could survey the landscape with fresh eyes.

Privileges:
Adopting a Modern Model

A common attack vector for cybercrime is privilege abuse. Corporate treasurers concur that managing entitlements and permissions in their banking platforms is a major concern.

The entitlement grid—who has access to which accounts and with what limits or guardrails—can be quite complex because they encompass scores of employees (hundreds, if not thousands) and can include multiple accounts all of which might have different parameters.

Further, many organizations are using older mainframe systems, and have patched on new features over time, rather than replacing them or migrating to more effective cloud-based systems. As a result, these systems might be cumbersome to use. For example, they often require manual input for each new person added or de-commissioned.

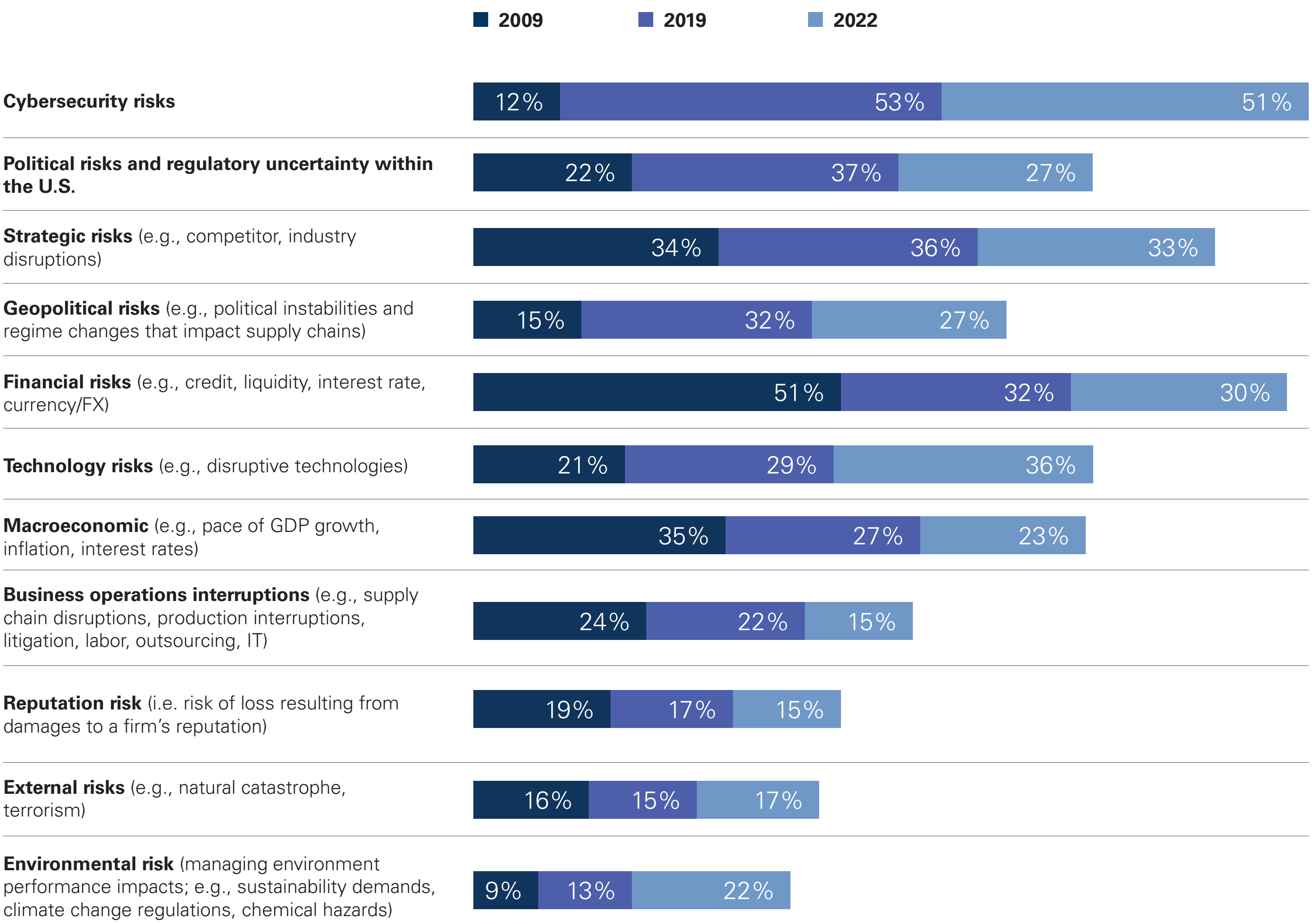
Tackling the issue of privileges might be facile at small organizations; limiting entitlements so users only get the bare minimum user privileges to do their jobs (a.k.a., the "principle of least privilege")—can be an effective step. That's not that simple at larger organizations, so we set out to explore paths that could make entitlement management seam-

Privileges: Adopting a Modern Model

less for the administrator and easier for end users. That's a big reason why we are embedding cloud-based automated provisioning and de-provisioning in our new transaction banking platform.

Another process we are adopting in employing a modern approach is migrating away from the entitlement grid where an administrator is forced to map out permissions for every person in their organization one-by-one. Instead, we have built out a process where each time a new user is brought on board, that user simply inherits the default permissions that were set up by the treasury at account opening. It's a unique blend of control, visibility, and ease of use. This way the process of creating entitlements literally is checking a box and adding

Ranking Risks
Risks that were/are/will be the most challenging to manage (percent of respondents who rank risks in top three).



Source: *2020 AFP® Risk Survey*, Association for Financial Professionals.

(or subtracting) someone from a list—and immediately transferring all of the limits and guardrails that were associated with that account.

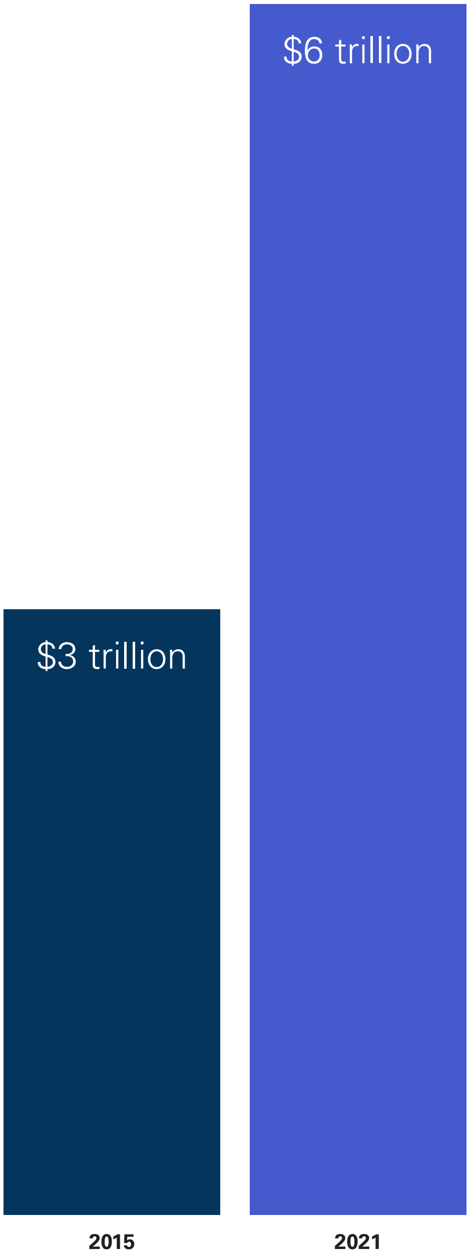
While this might seem trivial, it can save an enormous amount of time, as an administrator no longer has to create an account from the ground up, adding granular details about payment rails, daily limits, account access parameters, and other information). If an employee mandates a unique entitlement (say a CFO who needs access to everything and reduced limits), exceptions can be made.

In our experience, the differentiated entitlements system with exception management is far easier to implement than having to input every detail manually. And, coupled with a cloud-based automated provisioning system, it can reduce many of the issues of dealing with privileges. Goldman Sachs' transaction banking platform will employ both these measures in its efforts to make privilege management easier and more secure. ■

> **In our experience, the differentiated entitlements system with exception management is far easier to implement than having to input every detail manually.**

Crime Costs

Cybersecurity Ventures predicts that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.



Source: "Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021," *Cybercrime Magazine*, 03/29/2020.

Authentication: Moving to Advanced Tokens

Authentication is another major issue facing corporate treasurers—and, if not handled properly, can lead to compromised credentials and accounts.

The challenge is more important than ever; two of the largest data exposures of all time happened just last year,[4] underscoring the still-critical timeliness of securing user data.

It might be surprising, but adding protection beyond a user password, in the form of strong multi-factor authentication, is not widely used. In a 2019 report, the Ponemon Institute found that 55 percent of respondents do not use any form of two-factor authentication at work.[5] The report also found that managing passwords is time consuming; on average, respondents report spending almost 11 hours per year entering and/or resetting passwords, with an annual productivity hit of $5.2 million to a 15,000-employee company. Further, poor password practices are far more common than it should be—research shows that 73% of passwords are duplicates and 81% of breaches involve stolen or weak credentials[6]—which can lead to phishing attacks.

To combat these threats, more than half of the respondents in the Ponemon survey want more security, including 56 percent who see hard tokens as the answer. But this approach, which involves physically storing and cataloging thousands of units and then shipping the tokens to users via mail, is not without shortcomings. The process not only raises costs (the maintenance of the physical tokens) but also adds to time (shipping the units could take up to five days). And it raises security issues, such as lost mail or compromised shipping. Other options, such as one-time passwords sent via SMS, remain prone to phishing and other vulnerabilities.[7]

We believe the most appealing option at the present time (and the one we are implementing) is a soft-token, multi-factor authentication strategy. First off, all the factors attached to hard tokens—time, cost and theft—are mitigated by soft-tokens. A soft-token resides in the hands of the user, and this eliminates the so called "man-in-the-middle" who can intercept and compromise the physical token. Soft tokens are stored on and activated by a general-purpose electronic device—a desktop computer, a laptop, a PDA, or a mobile phone. Registering a soft-token procured by the client only takes minutes—reducing lag times to get a user activated.

The use of tokens as a multi-factor authentication method is fairly well established in large corporations, and the early reports are encouraging, to say the least. Google, for one, reports that its adoption of tokens has eliminated—not just reduced—phishing and man-in-the-middle attacks.[8] While Google uses a hardware-based token in its efforts, we see soft-token multi-factor authentication providing the same robust security features, and that's why it's being deployed in Goldman Sachs' transaction banking platform. ■

We believe the most appealing option at the present time (and the one we are implementing) is a soft-token, multi-factor authentication strategy.

Conclusion: Encouraging Positive Change

There's a natural and even understandable behavioral resistance to change. There's also an assumption that having a paper-based process (wet signatures, and the like) is the safest route. But those systems prove to be not as secure as users expect, they lead to calcified internal processes, and, most importantly, they disrupt corporate treasury departments and keep them from focusing on more value-added responsibilities.

Goldman Sachs' new transaction banking platform seeks to address these shortcomings by employing modern, leading-edge security technology that strengthens safety processes and reduces or even eliminates the complexity of corporate banking. Much in the way that digital apps have made consumers' daily lives better, corporate treasurers benefit by having a single, seamless global payments platform to handle their reporting, entitlement, and calculations. "Ease of use" isn't an expression you hear all that often when it comes to technology deployed in corporate treasury departments. At least until now. ■

[1] *2019 AFP® CYBERRISK SURVEY*, Association for Financial Professionals. | [2] *2020 AFP Risk Survey*, Association for Financial Professionals. | [3] "Top 5 Cybersecurity Facts, Figures, Predictions, And Statistics For 2020 To 2021," *Cybercrime Magazine*, 03/29/2020. | [4] "Hackers have become so sophisticated that nearly 4 billion records have been stolen from people in the last decade alone. Here are the 10 biggest data breaches of the 2010s," Business Insider, 11/13/2109. | [5] *2019 State of Password and Authentication Security Behaviors*, Yubico. | [6] *3 Common Mistakes That Lead to a Security Breach*, Okta. | [7] *Security Keys: Practical Cryptographic Second Factors for the Modern Web*, Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas, Google, Inc. | [8] Ibid.

Transaction Banking is a business of Goldman Sachs Bank USA ("GS Bank") and its affiliates. GS Bank is a New York State–chartered bank and a member of the Federal Reserve System and FDIC, as well as a swap dealer registered with the CFTC, and is a wholly owned subsidiary of The Goldman Sachs Group, Inc. ("Goldman Sachs"). Transaction Banking services leverages the resources of multiple Goldman Sachs subsidiaries, subject to legal, internal, and regulatory restrictions. Transaction Banking has engaged a third party to participate in the research and preparation of this material.