Recent high-profile cases of deplatforming by technology providers have made executive leaders aware of this growing business risk. Leaders should investigate the risk of deplatforming in their own organizations and choose an approach to mitigate it.

**Overview**

**Impacts**
- Any technology platform provider can deplatform your enterprise if it wants to.
- Businesses increasingly depend on technology platforms they don't control.
- Mitigating platform risk is a board-level responsibility.

**Recommendations**

Executive leaders guiding digital business should:

- Assign a staff member or small team to monitor the acceptable use policies (AUPs) of contractual and noncontractual platform providers and create a monthly update on any changes.
- Calculate a threshold for investing in risk mitigation by multiplying the potential costs of being deplatformed against the probability of this occurring.
- Develop proposals for mitigating the risk of deplatforming based on the risk threshold and four levels at which replatforming can occur (individual, enterprise, industry, country). Ask the CEO to present them to the board of directors.
Introduction

Deplatforming could have serious consequences for the enterprise, but the risk has crept up on executive leaders. The enterprise has slowly shifted business and operations onto technology platforms it doesn't control, including:

- Software as a service (at all levels of the technology stack) and hosted apps
- Cloud infrastructure and platform services
- Other hosted and outsourced services
- Marketplaces
- Social media
- Payments
- Industry ecosystems
- Internet of Things

Deplatforming has become more visible today as powerful entities are now being affected. For example, in February 2021, Facebook pulled out of Australia overnight to protest a new law requiring social media platforms to pay royalties when it shares news stories. Jurisdictions in Australia relied on Facebook for communications around health, emergencies and other public priorities. This and other incidents highlight that technology platform providers can deplatform anyone almost at will and that they are increasingly responsive to changeable political sentiment (see Figure 1 and Note 1 for deplatforming examples). Executive leaders should consider three impacts of deplatforming in order to decide how to mitigate the risk.
Figure 1: Recent Examples of Deplatforming

**Recent Examples of Deplatforming**

<table>
<thead>
<tr>
<th>Year</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>Daily Stormer deplatformed</td>
</tr>
<tr>
<td>2018</td>
<td>Domain registrars drop Gab</td>
</tr>
<tr>
<td>2019</td>
<td>Salesforce stops enabling sale of firearms</td>
</tr>
<tr>
<td>2020</td>
<td>Credit card companies drop Pornhub</td>
</tr>
<tr>
<td>Jan. 2021</td>
<td>Parler removed from Apple and Google app stores</td>
</tr>
<tr>
<td>Jan. 2021</td>
<td>70,000 social media accounts closed after U.S. Capitol riot</td>
</tr>
<tr>
<td>Feb. 2021</td>
<td>Facebook pulls out of Australia</td>
</tr>
</tbody>
</table>

Source: Gartner

Impacts and Recommendations

A Technology Platform Provider Can Deplatform Your Enterprise If It Wants To

Technology platform providers can determine that a customer is undesirable for a number of reasons, including:

- Worry that the customer is, or will become, a competitor
- Need to reduce civil or criminal liability caused by the customer’s actions
- Desire to combat fraud or abuse committed by the customer’s employees or a third party using its systems
- Conflicts of interest that show anti-competitive preference for partners where there is an existing financial interest
- Concern about political or social backlash related to the customer’s business
- Response to a change in law
All of the above circumstances can change rapidly, especially the last two. If a platform provider wants to stop serving a customer it can do so in a few ways:

- Simply drop the customer if there isn’t a contract or if there’s a termination for convenience provision
- Not renew the contract if there is one or make an unattractive renewal offer
- Cite a violation of the acceptable use policy (AUP)

Many enterprises do not think through the implications of the AUP, as they assume that they would never knowingly violate it. The often well-meaning language of AUPs leaves scope for subjective interpretation — for example, terms against bigotry, privacy violations, unwanted communications and false information.

Where customers sign a contract, the AUP is linked via URL, and the vendor can typically change the AUP at will. If there’s a termination for convenience provision, the vendor could terminate a contract at very short notice (possibly as little as 30 days). Many enterprises have no or scant exit plan, so that is a large risk.

Moreover, deplatforming by one vendor can start a cascade of other vendors deplatforming the enterprise.

Recommendations:

- Direct staff to review the terms and conditions of the AUP before signing a contract or entrusting a critical part of your business to a platform provider.
- Assign a staff member or small team to monitor the AUPs of (contractual and noncontractual) platform providers and to create a monthly update on any changes.
- Seek quarterly reports from vendor management teams on how well platform providers have delivered against claims.
- Ask the public relations or corporate communications team to provide a quarterly briefing on political sentiment and risks around the enterprise and its business or industry. These can act as an early warning for deplatforming.
Businesses Increasingly Depend on Technology Platforms They Don’t Control

Most executive leaders do not understand how dependent the business is on technology platforms. Mostly, leaders leave relationships with platform providers to vendor management professionals — or to no one if the enterprise uses public platforms, such as social media, without contracts. However, even professionals may not understand the business implications of platform relationships. Operational details can suddenly take on huge significance. For example, SolarWinds left it to an intern to change the password on its update server, and the failure to do so opened the way for a cyberattack that affected 9 U.S. government agencies and 100 private-sector organizations.

Although the risk of deplatforming remains small, the growing number of platforms enterprises use and the businesses’ growing dependence on platforms increase the consequences of deplatforming. Therefore, leaders should conduct a risk assessment, based on the nature of their business.

Recommendations:

- Incorporate the definition of key terms from AUPs (or other sources linked to contracts by URL) into an appendix to the contract (or at the very least, download copies at time of signature).
- Make explicit in the contract the activities that the business performs and that the provider agrees these activities are not a breach of particular AUP definitions.
- Add language to the contract that URL-linked policies, order forms or any other agreement subsequent to the contract will not materially diminish the terms of service of the original contract.
Mitigating Platform Risk Is a Board-Level Responsibility

The use of platforms usually ties directly to top-level strategic objectives, such as digitalization, speed to market and cost reduction. Thus, platforms play a role in a business strategy with assumptions the board of directors has signed off on, including budgets. Mitigating the risk of deplatforming probably requires the board to reconsider those assumptions.

Recommendations:

- Calculate a threshold for investing in risk mitigation by multiplying the potential costs of being deplatformed against the probability of this occurring:
  - Commission an inventory of all cloud platforms used by your business unit and which business activities depend on them.
  - Determine the costs to the business if one of the providers deplatformed you.
  - Examine any links to other platforms that could cause a deplatforming cascade.
  - Evaluate the probability of deplatforming by looking at four levels:
    - Individual — A senior leader or influencer in the enterprise is deplatformed for something he or she said or did.
    - Enterprise — The enterprise is deplatformed because of its behavior or for competitive reasons.
    - Industry — Technology platform providers stop doing business with all companies in a given sector.
    - Country — Platform providers pull out of a region for business or political reasons.

- Recommend to the CEO that all business units perform similar risk assessments.
Develop proposals for mitigating the risk of deplatforming, based on the risk threshold and the four levels. Possible approaches include:

- Developing an early-warning function for the enterprise to spot changes in internal and external circumstances that might lead to deplatforming
- Reviewing platform relationships and business dependencies periodically at a high level (e.g., board or CEO)
- Splitting work between platforms so that the enterprise can quickly shift work to a different platform if one provider deplatforms it
- Building and running your own platform
- Working with other organizations to lobby for regulations on deplatforming. Governments may be receptive to such proposals after Facebook's pull-out from Australia.

Ask the CEO to present these proposals to the board. They may require a change in strategy (e.g., from minimizing costs to minimizing risk) and new investments.

Note 1: Recent Examples of Deplatforming

- In January 2021, Facebook, Twitter and other media companies banned tens of thousands of accounts, including U.S. President Donald Trump's, for spreading lies and disinformation.
  
  Apple and Amazon removed social media app Parler for the same reason.

- In 2020, credit card platforms stopped doing business with Pornhub.

- In 2019, Salesforce refused to enable retailers to sell firearms on its platform.

- In 2018, Gab's domain naming and payment platforms removed the social media site.

- In 2017, “The Daily Stormer” was deplatformed by domain registrars.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

What Is the Risk of Actually Losing Your Cloud Provider?