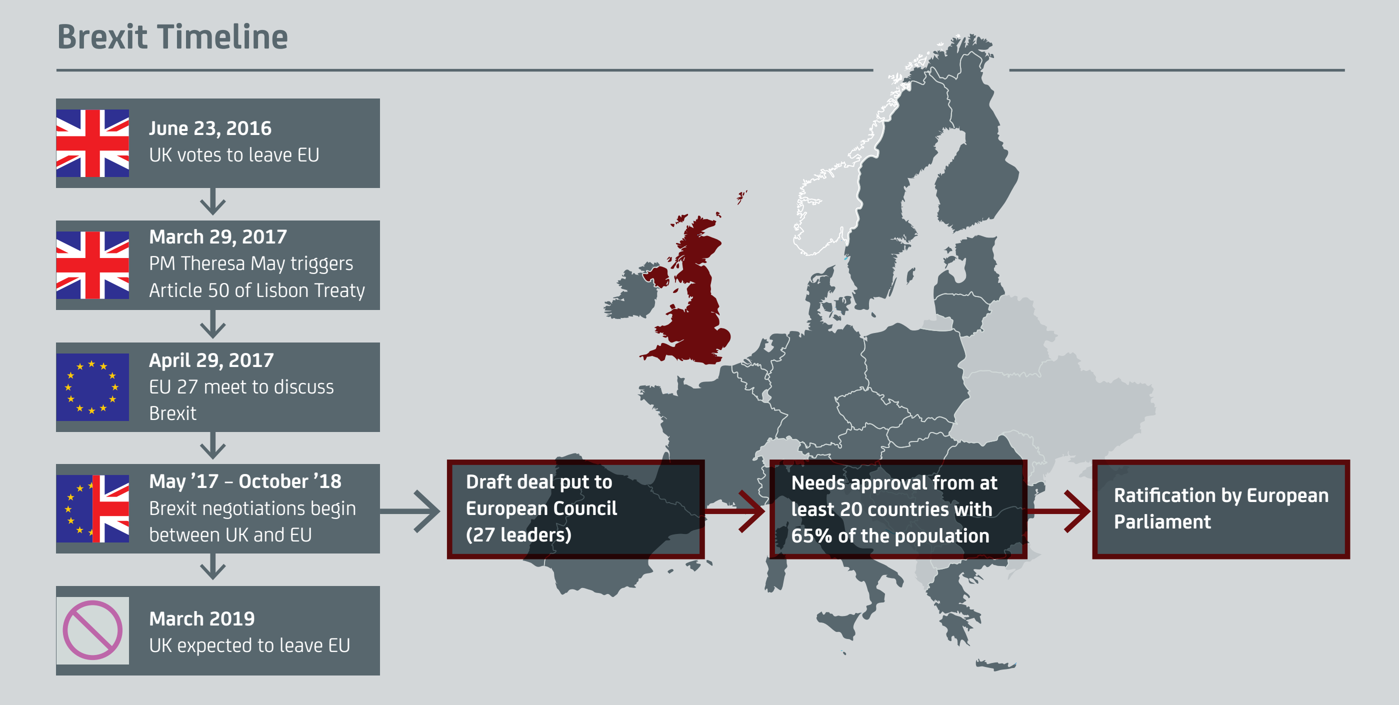
Brexit—The Impact on Privileged Identities

As the United Kingdom and the rest of Europe prepare for Brexit (Britain's exit from the European Union), information security experts are left wondering what this would mean to the security and risk management processes that have been put in place in the past and how they need to adjust to the emerging reality. This document discusses the impact of Brexit on privileged access management and what information security professionals may consider as immediate solutions to mitigate risks.

Brexit—What Happens Next?

With the formal notification of the United Kingdom (UK) leaving the European Union (EU) by Prime Minister Theresa May, the official process of leaving the EU has begun. There is now a 24-month window during which both parties need to create a framework to work together. The process is described in the diagram below.



Brexit Timeline

June 23, 2016
UK votes to leave EU

March 29, 2017
PM Theresa May triggers Article 50 of Lisbon Treaty

April 29, 2017
EU 27 meet to discuss Brexit

May '17 – October '18
Brexit negotiation begin between UK and EU

March 2019
UK expected to leave EU

Draft deal put to European Council (27 leaders)

Needs approval from at least 20 countries with 65% of the population

Ratification by European Parliament

Figure A. Brexit Timeline (Courtesy APA and DW)

Over the next 24 months, the EU and the UK must agree upon the terms of engagement after the split. Meanwhile, various public and private organizations on both sides have started to work out ways to conduct business in a smooth manner. This process is fraught with many blind alleys and risks. After all, everyone involved, both directly and indirectly, is navigating unchartered territory. This necessitates a well-thought-out risk management program.

Potential Economic Impact

There have been many models of the macroeconomic impact of Brexit on UK. Many of these suggest the following:

- Drop in GDP over the long term
- Fall in Foreign Direct Investment (FDI)
- Slowdown in immigration

Collectively, this means that many organizations will have to look at ways in which they can remain competitive and keep servicing their respective markets. To ensure minimal impact to the conduct of business, organizations are building a framework for the future, often taking the worst-case scenario into consideration. “For planning purposes, we must assume a ‘hard’ Brexit in which the UK loses its ability to passport into the EU,” wrote Citigroup’s European CEO James Cowles in a memo to staff. Other financial institutions have embarked on similar plans. But financial institutions are not alone. The impact on both sides of the breakup must be considered. For example, Vauxhall is thinking about sourcing its complete supply chain for the UK from within the UK, while BMW is looking for a new location in mainland Europe for its Mini. However, any rational business decision that impacts labor—for example, a move to improve productivity within the UK to reach levels of other EU countries, or changes in global demand—runs the risk of being labeled a victim of Brexit.

Impact on Jobs

One of the areas of concern will be the impact of Brexit on jobs. Various organizations have hinted at movement of jobs across borders—for example, Nestlé’s decision to move its Blue Riband chocolate-bar manufacturing from the UK to Poland may correlate with the elimination of 300 UK jobs. This may be a result of changes in the immigration environment (tightening of visa laws or greater scrutiny), or because of trade tariffs and uncertainty. Hiring in the UK private sector has dropped to its lowest level in three years owing to uncertainties around Brexit, according to one of the world’s largest recruitment firms. Such movement of jobs not only has a significant impact on the overall economy, but also poses a very high information-security threat.

Risk Exposure

As we have seen so far, there is ample evidence that there are important risks organizations need to manage as part of Brexit. Coupled with the dramatic technological changes we are witnessing today, IT risk management has assumed considerable significance. An important part of this happens to be information security risk. It is well documented that the greatest financial and brand risks for information security assets come from the exploitation of privileged-user access. This risk has amplified as organizations have adopted cloud and virtual environments for business growth and digital transformation.

Addressing Privileged Access Management Risks

As organizations consider their options for addressing the challenges presented by Brexit, specifically the movement of employees, they need to consider the risk of insider threats. Any uncertainty, such as potential changes in employment status or transfer of responsibilities, can lead to uncertain behavior from insiders. It also presents a malicious outsider with an opportunity to exploit potential vulnerabilities. Further, transfer of responsibilities, such as employing a third-party vendor for certain business functions, can lead to more exposure and will require proper oversight and visibility. These issues collectively call for a need to implement an effective privileged access risk mitigation strategy. In fact, protecting sensitive data and intellectual property becomes significantly important.

Considerations to Mitigate Privileged Access Risk

The following need to be considered to mitigate risk due to compromises or abuses of privileged access during uncertainty.

1. **Scale:** Surface of exposure
   a. Endpoints/devices: Not limited to data stored on-premises, but also any virtual and cloud based assets
   b. Identities: Not limited to just administrative users, but also any application-to-application accounts and scripts

2. **Scope:** Future strategy
    a. Digital transformation: If there is a digital transformation program, factor in any customers, vendors or partners participating
    b. Internet of Things (IoT) programs: Consider any device that may have access to privileged information
3. **Automation:** Machine learning and session recording
    a. Machine learning: Using user behavior analytics (UBA) to detect anomalies in order to reduce time to detect and mitigate exposure
    b. Session recording: Use for non-repudiation and compliance
4. **Resources:** Budget and talent
    a. Budget: Given the geopolitical uncertainty, it is very likely that budgets will be constrained while Brexit is being negotiated
    b. Talent: With the impending immigration changes and migration of talent, it will be important to ensure that the need for specific skills does not impede deployment

Conclusion

Privileged access management, such as solutions from CA Technologies, will be important in ensuring that critical assets are well protected during this phase of geopolitical change. While it may be appealing to consider starting with basic functionality, such as password vaulting, to mitigate risk, it is important to look at the problem holistically. Brexit has a fixed timetable. The pace of activity is likely to accelerate, giving information security professionals a very short time to react. It will be critical to consider the total cost of ownership (TCO) of a solution, along with the scope and scale of functional support, before embarking on this journey. Plan to encounter unknowns such as segregation of duties and data sovereignty issues during the process. Finally, consider a solution that not only provides scale, scope and automation, but also acts as the foundation of secure privileged access management, coupled with analytics driven by machine learning. This change impacts not just the UK, but also any significant trading partner of the UK and the European Union.