TEVORA™

Whitepaper | June 22, 2018

THE POWER OF A DIGITAL TRANSFORMATION

Ben Dimick, Manager of Information Security

tevora.com

TEVORA™

What is a Digital Transformation?

A digital transformation can refer to any change an organization makes to a process or business activity to fully utilize the opportunity and value of technology. Recently, this term is most used to describe changes that allow internal users, customers, partners, vendors, and others to interface more seamlessly. Many times, this involves creating a more immersive experience or allowing for easier and more reliable access to data. With the prevalence of mobile workforces and customer interaction from mobile clients, the mobile experience is another common component of digital transformations.

Regardless of the goals within the digital transformation, there are a few common components to most digital transformations. Defining and controlling **access** is one key consideration. Ensuring users and clients have a consistent experience across all platforms is crucial to convenient and secure interactions. Another component is **convergence**. As the number of systems used increases, the complexity for handling these systems also increases and the user experience can suffer. Finally, **automation** can spell the difference between success and failure. As more systems become connected and user experiences are intended to become more seamless, the effort to manage increases and the expected delay in obtaining access dwindles. Automation allows these two estimates to converge.

Access

Establishing access to resources is the clearest benefit of digital transformation for users, but implementing access securely can be challenging. Many security experts have claimed the use of the password is dead[1], but few organizations have been able to truly abandon the practice. Far fewer remove passwords from external users, such as B2C and B2B applications, and even those that do usually a password at some point during the chain to prove the identity of the user[2].

Digital transformations provide new options for authentication that improve user security and experiences. For instance, mobile applications have increased the capability of enterprises to implement new methods for authentication, such as device trust, one-time passcode, and push validation. The user experience can also be simplified. Microsoft has attempted to extend [3]cloud services to the desktop for years and recently added new device trust functionality to Office 365, which allows users to avoid entering passwords between sessions[4].

Whatever the appropriate method for perform authentication, the need for a unified login experience is becoming more important than ever. As more websites incorporate “Login through Facebook[5]”, “Google Sign-In[6]”, and other features, more businesses and online services are connecting accounts across platforms to provide a more seamless experience for clients. Linking profiles also results in improved analytics for businesses.

Convergence

A key factor of many digital transformations is the integration of various systems and processes. The advent of the internet provided several strong examples of this occurring, especially for traditional retailers. As customers began using the internet to access information, they began to demand inventory systems be tied to the website to allow the customer to understand if a product was in stock before attempting to purchase it in person. Further, the online purchasing system needed to integrate with internal shipping systems, so customers could buy a product online and then visit the store to pick it up instead of waiting for it to arrive via traditional methods of conveyance. These functions are generally considered standard for retailers now, but public demand continues to push for more features from companies they would do business with[7].

Incorporating systems that have not been connected previously introduces several challenges for organizations. Not only does this frequently require building new system functionalityit requires the creation of anew communication method. This

[1] https://www.scmagazine.com/opinion-the-password-is-dead/article/544185/
[2] https://www.technologyreview.com/s/510106/googles-alternative-to-the-password/
[3] https://docs.microsoft.com/en-us/windows/client-management/mdm/mdm-enrollment-of-windows-devices
[4] https://cloudblogs.microsoft.com/enterprisemobility/2017/09/19/fewer-login-prompts-the-new-keep-me-signed-in-experience-for-azure-ad-is-in-preview/
[5] https://developers.facebook.com/docs/facebook-login/
[6] https://developers.google.com/identity/
[7] https://www.thinkwithgoogle.com/marketing-resources/omnichannel/best-buy-digital-ads-in-store-sales/

leads to a variety of security concerns, including access controls, secure transport of data, and new data handling considerations. Implementing a consistent data classification and protection policy, as well as executing within the parameters set by it, is crucial for data security. These issues can be further complicated when personally identifiable information is exchanged.

Protecting new avenues for data flows can be a daunting task. Utilizing systems for purposes other than the original function will frequently introduce new challenges. Implementing an API access management system[8] can help alleviate some of the obstacles encountered as a result of these changes. As with all major changes in an enterprise environment, conducting targeted penetration testing[9] is advised to ensure secure implementation methodologies are observed.

Automation

As more systems are integrated, the overhead to maintain user access of those systems increases. This becomes even more problematic in the current landscape of instant access. With the user demand for instant access to information, delaying access for even a few minutes can result in the loss of a customer. The result is that integrated systems must not share only data, but user access seamlessly.

Automation can make the management of critical systems more secure and consistent, as they are less affected by routine human error. This also reduces system operating costs and begins to show real value. This is especially true of B2B implementations, where access needs to be controlled and revoked at various times. As an example of this growing into the business arena, Okta[10] announced a new feature for their cloud identity platform that allows users from one Okta instance to quickly and easily sign into another, thereby establishing a rapid trust between two organizations and allowing users access to those applications intended for their use.

Finding Success with Digital Transformations

As with many enterprise engagements, the key to success is early and formal planning. New features should be reviewed and evaluated for potential risks to the enterprise and to the initiative itself. Understanding how systems will integrate and the ancillary support systems involved is also crucial to success. Digital transformations can be a significant factor in business growth and offer cost savings, a seamless user experience, and increased security when properly executed. Tevora is a specialized management consultancy focused on cybersecurity, risk, and compliance services. Our combination of collaborative strategic planning and skillful execution make us a trusted partner to some of the most famous brands in the world.

[8] https://www.okta.com/products/api-access-management/
[9] https://www.tevora.com/services/threat-management/application-penetration-testing/
[10] https://www.okta.com/programs/sign-in-with-okta/

TEVORA™

Go forward. We've got your back.

We live in a digital world, and your customers trust you to keep their information safe. We make it our responsibility to equip you with the information, tools, and guidance you need to stay out of the headlines [and get back to business].

Eyes on the future.

Tevora takes a long-term outlook and proactive approach to every engagement. We combine our technical knowledge with practical business acumen to produce and execute strategies that fortify your organization's assets and build a foundation for the future.

Audit Standards

Our MBAs and CISSPs can help your organization assess and test against PCI DSS, PADSS, HITRUST, ISO 27001, STAR,
SOC I, SOC II, MPAA and more.

One Spectrum Pointe Drive
Suite 200, Lake Forest
CA 92630

12655 West Jefferson Blvd.
4th Floor, Los Angeles
CA 90066

205 East 42nd Street
20th Floor, New York
NY 10017

tevora.com