



The Benefits of Hyperautomation

By Nathan Hull, Principal Solutions Architect, Technologist

Hyperautomation – in short is the process of automating business automation. At least that is the goal. The term itself was coined by Gartner in 2019 and implies an actual framework for scaling business automation by combining complementary technologies to augment business processes. The benefits of hyperautomation extend beyond the simple cost savings of reduced overhead by automating tasks. Hyperautomation reduces the cost associated to implement business process automations and enhances the utilization of other technologies such as ML and AI within the organization. By increasing process efficiencies and boosting productivity there are many other tangible benefits. For example, improved customer perception of the organization by being able to increase the speed of product or service delivery. Hyperautomation also creates the opportunity for business and process improvement. As more workflows are digitized there is more data that can be collected, analyzed, and ultimately translated into more effective business decisions.

Foundation is key! If I could stress only one common component in the successful implementation of technology projects, it would be just that. Having mature business processes in place and having a crystal-clear vision of what a process should be prior to taking on any type of automation project is highly recommended. At the end of the day, business process automation typically mimics what an individual user would do to complete a set of tasks. If the individual performing the tasks being modeled is completing them incorrectly, it isn't going to be very beneficial for the organization. Having defined goals

and outcomes is essential for project success and implementing Hyperautomation is no exception. Business automation almost always encompasses multiple organizational units. For instance, there is typically need for IT governance and oversight as well in-depth insight from the process owner that is to be automated. Therefore, to be most effective the business must be the driver of adoption and have appropriate executive sponsorship to prevent interdepartmental challenges from hindering the success of the project. How well processes are understood by both or multiple parties and having well established inter departmental communication is critical. Identifying the appropriate automation tools to construct a hyperautomation framework is also an important factor. For instance, if there are regulatory or organizational compliance guidelines that must be met, having automation tools that can support those policies is obviously key in developing an appropriate solution.

Once an organization has a clearly defined use case for hyperautomation, it is a general best practice to initially limit the number of processes or tools to be automated. Trying to combine an excess number of tools or automate too many processes in a short time frame can prove to be extremely challenging and increase the potential for negative impact on an organization. As complexity increases so does the risk of project failure. Starting small and detailing success criteria can prove immensely valuable once you are ready to expand the scope of your hyperautomation project.

Hyperautomation security is an important consideration and should be evaluated accordingly based on the organizations security policy and any overarching regulations or compliance mandates. Security policies regarding business automation systems are generally more focused on access controls given the nature of the products themselves. The majority of the tasks are transactional, and it is uncommon for the systems to store data within the platform itself. However, the possibility of a malicious user gaining access to sensitive data via an automation tool is plausible. If a malicious user were to utilize the tool itself to gather sensitive data from automated actions the impact could be rather substantial. Regarding access controls, it is important to understand the difference in roles between the hyperautomation components as well the user roles they take on to complete the automations. As an example, the hyperautomation of HR onboarding does not necessarily require the automation components to have the same permissions as an HR employee. The HR employee will likely have a much more expansive role and access to many systems unrelated to those necessary to perform the onboarding tasks. Keep in mind that the permissions allocated to the automation systems should meet only the requirements to perform the expected tasks and nothing more.

Other security concerns may exist depending on the organization such as varying geographic regulations, privacy laws, etc.

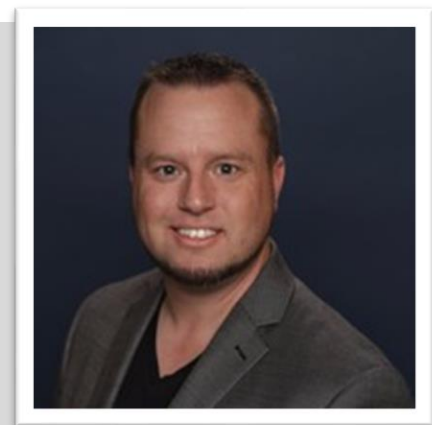
As with any system that is critical to business continuity, appropriate safeguards should be implemented to protect the business from system failure. Concepts such as high availability, disaster recover, etc., are an important factor when considering what role automation will have in your business. Setting appropriate service level expectations will assist in the supportability of the platform and assist in the adoption of these technologies.

Ultimately hyperautomation proposes a more complete path for organizations to realize the benefits of automation and will likely have a profound impact on multiple areas of business in the future.

About the Author

Nathan Hull, Principal Solutions Architect for Technogent.

With more than 15 years industry experience Nathan works with clients as a transformational IT consultant. He assists organizations in solving strategic, operational, and technological challenges. Carrying a reputation for motivating and inspiring teams through the well-organized, efficient implementation of emerging technologies.



Nathan can be reached online at on the company website <http://www.technogent.com/>



CYBER DEFENSE MAGAZINE

eMAGAZINE

**DECEMBER
2 0 2 1**

In This Edition

9 Ways Social Media Sabotages Your Cybersecurity

How Covid-19 Changed Advertising Forever

The Benefits of Hyperautomation

Why Do You Need a Malware Sandbox?

...and much more...

MORE INSIDE!