Robotic Process Automation

IntelliDyne®
EXPERIENCE ABOVE & BEYOND

Getting the Most Out of Your RPA Initiative

There has been a lot of buzz recently around the promise of Robotic Process Automation (RPA). If you're a technology executive and you're not familiar with it, you should be. In the current federal fiscal cost-cutting climate of doing more with less, RPA should be on your short list of technologies to check out. And it doesn't hurt that it's just...well, cool.

Robotic Process Automation enables you to create software robots ('bots") to automate just about any of your business processes. They can interact with your systems or applications the same way you do. Bots can learn. Using technology that mimics human behavior to interact with existing human system interfaces, RPA essentially allows the creation of a virtual digital workforce, capable of performing simple to complex repetitive data entry or data movement tasks and business processes. These virtual workers are immune to the typical factors that may prevent salaried workers from accomplishing their work, be it vacation, illness, jury duty, or furlough. To be clear, we are not talking about job elimination; we are simply talking about freeing employees from high volume, error prone, repetitive tasks to work on higher-order, more important, or even more satisfying work.

Using technology that mimics human behavior to interact with existing human system interfaces, RPA essentially allows the creation of a virtual digital workforce.

For example, during a site visit to our largest Defense client, I was approached by a mid-level security engineer who literally begged for a solution to relieve the daily pain caused by a process to identify and mitigate security vulnerabilities on end-user devices. This single task is full of time-wasters that includes the opening of multiple applications to identify, patch, and secure each vulnerability...all of which is painfully rewarded with a requirement to manually produce multiple reports documenting the activity.

This critically-necessary (but time-consuming) task is a complicated cross-analysis of four detailed data sources (DISA's Assured Compliance Assessment Solution [ACAS], Microsoft's System Center Configuration Manager [SCCM], ePO/McAfee, and Active Directory [AD]) – all to identify active security risks and create tickets in the BMC Remedy system to patch or take a device offline. Keep in mind, this is an enterprise with a few hundred thousand end user devices, but this engineer's area of responsibility covered only about six-thousand of those devices...meaning that multiple personnel elsewhere in the enterprise are performing the same convoluted, manual processes, sacrificing additional efficiency – the problem has scale.

This was the use-case that launched our RPA initiative. It uses a simple artificial intelligence (AI) process to automatically launch the SCCM and ACAS scans and pull data from AD and McAfee/ePO to cross-correlate devices, users, and vulnerabilities – identifying potentially out-of-compliance devices. We embedded the security engineer's business rules into the process to identify and select those issues to be entered into the incident management system. Then, the virtual worker (the RPA) 'logs in' and navigates to the correct Remedy screens to create individual tickets for each device requiring attention. The virtual worker 'logs' into each system to perform each of the separate tasks, chaining them all together to form a 'virtualized process'.... all without writing procedural code to interface with any vendors' system application program interfaces (API). The 'virtual worker' works 24/7 365 days per year. In our example, the security engineer recaptures valuable time that can be used for more complex, non-manual tasks, directly impacting organizational effectiveness, increasing productivity, and corralling costs.

If you're considering launching your own RPA initiative, the first step is to identify manual processes that will yield the greatest benefit when automated. Thoroughly documenting the current process – to later compare it with the end result of RPA – will provide the clarity needed to make the decision to continue any RPAs after your initial pilot project. When organizational and economic impacts are quantifiable, 'yes' becomes much easier.

The below guidelines are just a few of the criteria you may find useful to help narrow the selection of candidate use cases in your organization. A word of advice would be to ensure that your candidate use cases follow rules-based logic with relatively few exceptions and that these processes don't change regularly.

Let us know if you're considering an RPA initiative and would like to discuss a roadmap for getting there.

Here are a few guidelines to follow when deciding which processes to automate with RPA in your organization:

HIGH COST IMPACT—Most impactful processes are expensive and touch customers. In our IT security example above, determining high-risk vulnerabilities required touching thousands of 'customers' or, end-users. The expense can be easily determined by scaling the cost of the engineers' activity across the enterprise, 50x in our example. Such processes are great candidates for RPA if they can be automated. The ROI and payback period can easily be determined in this example– which made the economic argument all the easier

HIGH REPETITION/VOLUME—One of the key benefits of RPA is the reduction of highly repetitive human effort. Repetitive data tasks at volume may be an indicator of low-order activities that can be automated. Have your staff look for candidate use-cases within your organization. You should consider automating your highest volume processes first.

ERROR-PRONE PROCESSES—Multi-step manual processes are, by nature, more prone to human error. Combine this with a high-volume scenario, and you will find employees that are experiencing process-fatigue, distraction, and inattentiveness —all of which lead to an increase in the probability of error. Combine these criteria with use-cases that have a low tolerance for error, and consider the impact that automation could have on lowering enterprise risk or improving the end-user relationship/experience.

LOW TOLERANCE FOR ERROR—In many instances, manual mistakes or oversights can introduce risk, as in the case of our security compliance example, or even create regulatory problems as in consumer finance or healthcare use-cases. Automation will likely reduce the probability of error in most cases, by routinizing decision logic or eliminating keystroke errors.

TIME-SENSITIVITY—Procedural backlogs that delay the delivery of services to end users or delay the notification of risk events are great candidates for automation. In our security example, it would be impossible for the engineer to focus 100% of his time and attention to searching for vulnerabilities, not to mention the fact that we humans need a break now and then. Our 'virtual security engineer' is constantly, and tirelessly, watching, processing, and reporting security vulnerabilities.

LABOR ELASTICITY—When was the last time you asked an employee to only work for 25% pay this week but not to worry because they'll be able to make it up over the holiday? Processes that have wide demand variation force organizations to either over- or under-hire. With the advent of the cloud, we're all now sold on the value of elasticity when it comes to disk storage, or computational demand. Why not have that same elasticity in your manual processes? RPA-enabled processes allow you to scale up or down, regardless of peak demand or its timing.