EisnerAmper

EisnerAmper LLP
Accountants and Advisors

eisneramper.com

PRTS Intelligence

A publication from EisnerAmper
Process, Risk and Technology Solutions

Robotics (RPA) as a Service 2

Never Too Small for a Data Breach 5

Robotics (RPA) as a Service

By Ryan Zullo with an additional contribution from Caroline Keane

To help facilitate the need for dynamic growth, many organizations have adopted new business strategies, one of the most prominent among them being the move to "the cloud." Through greater efficiency gains and the realization of lower costs, cloud-based services are now starting to become the standard as small to midsized organizations around the globe are able to fully embrace them. Due to the prevalence of cloud-based services, it has become even more important for organizations to efficiently share and utilize their information, resources, and software to remain competitive. One solution that has enabled organizations to achieve high levels of efficiency is Robotics Process Automation (RPA). To fully appreciate how RPA can be leveraged in a cloud environment, one must first obtain an understanding of the cloud.

SO WHAT IS "THE CLOUD?"

In its simplest form, "the cloud" refers to cloud computing, which is the on-demand storing and retrieval of data and applications over a shared network instead of locally on an organization's own hardware. It is important to note that applications and data that are stored and run off someone else's local hardware are not considered as cloud computing. In order to qualify as being "in the cloud," applications and their comprising code, as well as their supporting infrastructure, must be delivered and run over the internet (Kohgadai). The applications and data, which are stored on the physical servers in a cloud network, are controlled and maintained by a cloud computing provider (What Is Cloud Computing & How Does It Work?). As users, an organization's personnel are able to access their applications and data stored on a cloud network. An example of this would be with Microsoft and its Office365 platform. Microsoft allows users to save their data on their servers as well as utilize versions of their applications (e.g. Excel, PowerPoint, Word, etc.) that are hosted on their end. Users, in turn, are able to access their data and Microsoft's applications at any time, as long as they have an internet connection.

To understand how the cloud works, it can be broken down into two parts, the front end and the back end. The front end of the cloud is the part that users see and can interact with. It includes an organization's computers and the applications required to access the cloud computing environment. Some cloud systems are accessible via dedicated applications while others are accessible through web browsers (e.g., Google Chrome, Mozilla Firefox). The back end of the cloud is comprised of the various applications, computers, data storage systems (e.g., hard drives), servers, and virtual machines that constitute and support the cloud computing service itself. The back end also provides the network, security, and traffic protocols that ensure connectivity with the front-end systems of which users interact (Strickland).

There are several advantages to the cloud computing model, the first being that it allows organizations to provide powerful and sophisticated applications to users simultaneously on a global scale. Without the need to install software locally, the cloud allows for the faster provisioning of applications and services, in many cases instantly, which allows for flexibility in when/where users can work. This is especially beneficial in a business continuity-type situation as having data stored in the cloud minimizes recovery point[1] and time[2] objectives, allowing for normal business processes to be resumed with internet connectivity. Coupled with a pay-per-usage model, the cloud also significantly lowers organizational costs as it eliminates, or at the very least reduces, the necessary investment on large-scale infrastructure and software to host and support local applications. This, in turn, allows for the reusability of IT resources and staff, enabling them to focus their attention on other facets of IT, such as research, development and critical support functions.

With some background of how the cloud computing model works, it is now important to gain an understanding of RPA to fully appreciate how it can be leveraged in a cloud environment to realize greater efficiencies.

ENTER THE ROBOTS

RPA is the application of specialized computer programs (i.e., "robots") to automate and standardize repetitious, rule-based business processes in both the back and front offices. While RPA does not involve any physical robots, the software itself is able to emulate human actions. To do this, RPA relies upon the existing technologies of artificial intelligence (AI), machine learning, neural networks, screen scraping, and workflow automation, elevating and advancing the sum of their individual capabilities. Through the utilization of these technologies, RPA robots can interact with existing application user interfaces to capture data, interpret actions, trigger responses and communicate with other systems and/or robots. RPA is able to accomplish all this in a non-intrusive manner as the robots themselves are self-contained and leverage an organization's existing IT infrastructure without causing disruption to the underlying systems – which would be costly to replace (Robotic Process Automation (RPA)).

Unlike their flesh-and-blood counterparts, robots are able to work 24/7/365 without succumbing to boredom, fatigue, or time constraints. Once properly trained, robots can operate a process the same way without deviation, eliminating the risk of human error while achieving high rates of efficiency. This is especially advantageous for organizations that rely upon a large labor force to perform extensive amounts of transactional processes as these types of tasks are, more often than not, undertaken with little interest by workers and, thus, suboptimal vigilance is deployed when performing them (Learning). According to data collected by Smartsheet Inc., a collaboration work management software solution provider, "nearly 60% of workers estimate that they could save six or more hours a week with automation" by eliminating productivity-killing tasks resulting from manual data collection/entry/syncing, approvals processes, and information requests/status updates (Beloof). By implementing robots and saving employees from these insistent tasks, organizations can optimize their workforce, redirecting workers toward more critical functions that require decision-making skill sets. This leads to increased overall work product throughout and reductions in operating costs. In some cases, robots may even be capable of entirely replacing their human counterparts.

While it is easy to get excited about the potential benefits and value that robots can deliver, it is just as easy to overlook the necessity of building out a robust RPA implementation strategy. Many organizations believe that once robots are set up, they can continue to run

[1]Recovery Point Objective is the amount of time prior to a disruption for which the lack of backed up data is acceptable
[2]Recovery Time Objective is the amount of time allowed for the restoration of a business processes in order to avoid unacceptable consequences from a severe disruption

autonomously without oversight; this is entirely untrue. Though they may leverage an organization's existing IT infrastructure, robots introduce an additional layer of complexity to the technology architecture that requires governance and oversight by IT (Sohoni). Robots also require constant management and maintenance over their lifetimes. The platforms that robots interact with are subject to change, and often the flexibility to deal with changes to the application user interfaces they interact with isn't configured accordingly; minor changes to an application form, for example, could throw off months of work (Boulton). Additionally, RPA can't fix poorly designed/broken processes. Rather, it speeds them up and shifts the resulting errors and bottlenecks further down the production line, which only creates deeper problems (Trefler). As a result, successfully building and deploying robots has proven to take a lot longer and be more complex and costly than many organizations ideally envisioned.

A NEW PARADIGM

There is good news, however. Many of the aforementioned difficulties encountered by organizations when setting up robots can be mitigated in a cloud environment. RPA delivered on the cloud is an example of a SaaS-based (Software as a Service) solution[3] as the infrastructure, maintenance, and support are being provided as services by the RPA vendor. What this means is that organizations are freed of the burdens of installation and ongoing administration of the robots (RPA). With minor configuration changes, organizations can directly deploy robots to perform specific tasks as the RPA vendor has already gone through the lengthy development process on their end. The cloud also enhances the capabilities of the robots as they are no longer limited by local resources in terms of computation power, memory and software. This allows them to grow and learn much faster than if they were installed locally. Furthermore, leveraging the vast infrastructure of a cloud-hosted environment allows robots to share data and perform powerful computations on a scale previously unprecedented, resulting in operations and tasks occurring within a fraction of the time required by that of locally installed robots.

LOOKING TOWARD THE FUTURE

The cloud has undoubtedly revolutionized the business landscape and changed it for the better. It has allowed organizations to gain access to more powerful applications and share information on a global scale. Looking for other means to gain further efficiencies, many organizations have begun to turn to RPA. RPA implementations, which are supported by extensive planning and robust design, have been proven to produce much stronger results. However, the continued maintenance and support of the robots created still falls upon the organizations themselves. Organizations that combine RPA with the cloud are not only able to free themselves of this burden, but also experience the benefits and realize value much faster than those that don't.

Ryan Zullo is a manager in EisnerAmper's PRTS. Questions? He can be reached at 347.735.4684 or ryan.zullo@eisneramper.com.

References

- *Beloof, Katy. How Much Time Are You Wasting on Manual, Repetitive Tasks? n.d. <https://www.smartsheet.com/blog/workers-waste-quarter-work-week-manual-repetitive-tasks>.*
- *Boulton, Clint. What is RPA? A revolution in business process automation. 03 September 2018. <https://www.cio.com/article/3236451/what-is-rpa-robotic-process-automation-explained.html>.*
- *Kohgadai, Ajmal. What is a Cloud Service? n.d. <https://www.skyhighnetworks.com/cloud-security-blog/what-is-a-cloud-service/>.*
- *Learning, AI & Machine. How RPA Assisting Businesses in Scaling Operations. 24 April 2019. <https://www.technative.io/how-rpa-assisting-businesses-in-scaling-operations/>.*
- *Robotic Process Automation (RPA). n.d. <https://www.uipath.com/rpa/robotic-process-automation>.*
- *RPA, CiGen. Robotic Process Automation (RPA) for Cloud Applications. 6 December 2018. <https://www.cigen.com.au/cigenblog/robotic-process-automation-rpa-cloud-applications>.*
- *Sohoni, Alex Edlich and Vik. Burned by the bots: Why robotic automation is stumbling. 24 May 2017. <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-blog/burned-by-the-bots-why-robotic-automation-is-stumbling>.*
- *Strickland, Jonathan. How Cloud Computing Works. n.d. <https://computer.howstuffworks.com/cloud-computing/cloud-computing1.htm>.*
- *Trefler, Alan. The Big RPA Bubble. 02 December 2018. <https://www.forbes.com/sites/cognitiveworld/2018/12/02/the-big-rpa-bubble/#4c9f5c1868d9>.*
- *What Is Cloud Computing & How Does It Work? n.d. <https://www.fastmetrics.com/blog/tech/what-is-cloud-computing/>.*
- *What Is Cloud Computing & How Does It Work? n.d. <https://www.fastmetrics.com/blog/tech/what-is-cloud-computing/>.*

[3]Software as a Service (SaaS) is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet. The provider gives customers network-based access to a single copy of an application that the provider created specifically for SaaS distribution. The application's source code is the same for all customers and when new features or functionalities are rolled out, they are rolled out to all customers.

Never Too Small for a Data Breach

By Tyler Dwyer

It seems as though nearly every day you hear about a business that has fallen victim to a data breach or other cyber-related incident. Companies of all sizes and industries are falling victim to the increasing threat of cyber-related crime. This has largely been due to the vast amounts of valuable data available within the networks and programs of organizations. Cybercriminals are continuously learning and developing new ways to obtain confidential data at a pace much faster than business owners are adapting to the changing risk landscape. There are a number of methods attackers employ to infiltrate an organization's systems to act maliciously. This makes deciding on the most useful tactics to mitigate the risk from the highest threat areas rather difficult. If you are a business owner, large or small, slow down and ask yourself if you have done everything to protect your organization, your data and yourself from the growing likelihood of a breach.

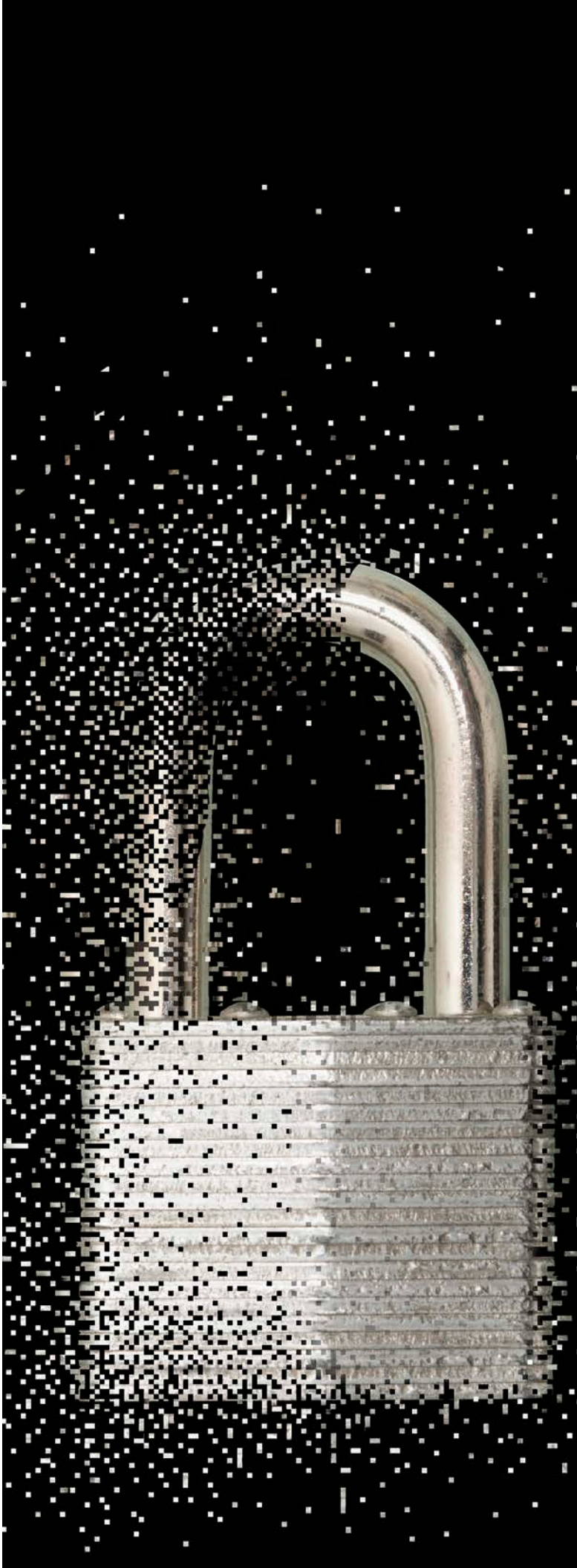
Last year alone, there were more than 1,300 data breaches reported publicly by large corporations. From only the sheer number of large organizations that have reported their breaches, this averages greater than three cyber-attacks per day. This total does not even consider the number of small to mid-sized organizations that have experienced a breach or larger organizations that have fallen victim but did not release this information publicly. The question of why these breaches and losses are becoming so frequent should be raised amongst management.

- Is this because of the growing knowledge base of malicious attackers who are finding an increasing number of targets to exploit?
- Is this due to a lack of employee understanding of cybersecurity practices and not realizing what is at risk?
- Is cybersecurity protection and loss prevention too expensive and time consuming to implement?
- Do business owners think they will not be targeted based on their size, business model complexity, and/or industry?

To be on the receiving end of a data breach is an unfavorable position and one every business owner would like to avoid. For every method used to gain unauthorized access to a business' data, there are just as many justifications a business can give as to why the breach occurred. One of the first steps to mitigate these threats and avoid a breach is to recognize the means by which cybercriminals can penetrate your business.

In order to determine the methods to employ to reduce the risk of a data breach in your business, first obtain a better understanding of the leading threat actions. Based on statistics from the *2018 Verizon Data Breach Investigations Report*, the top cybersecurity threats are as follows:

1. **Hacking –** A broad term to define the illegal usage of programs and tactics to obtain confidential and private user information including, but not limited to:
   - Cookie theft where usernames, passwords, and other information from your browser's history are stolen.
   - Denial of service attacks where sites and servers are flooded with traffic and overloaded causing a crash.
   - Keylogging where the activity, key strokes and sequences of your keyboard are monitored in an attempt to repeat a user's keystrokes to obtain confidential information.
2. **Malware –** Malicious code that infects a user's computer and allows a cybercriminal to gain illegal access to various functions. Two of the more common types of malware include:
   - Computer viruses that replicate on the host system and infect programs, files and other data.
   - Ransomware where company data has been compromised and is held hostage for a cash ransom by the malicious party.
3. **Social Engineering –** The most common being phishing, when a user is tricked into offering personal information to an unauthorized party through disguised email correspondence. More recently, phishing emails have embedded malware making it easier for the malicious party to gain access to confidential information.
4. **Human Error –** The unintentional act of losing or putting information at risk by allowing data to be obtained by unauthorized parties. This could be due to negligence, carelessness or lack of education on the subject.
5. **Physical –** The act of gaining confidential information through physical means such as:
   - Eavesdropping on conversations discussing private or confidential information.
   - Observing a user access their workstation to obtain their login credentials.
   - Unauthorized individual maliciously following an employee with special clearance into a restricted area
   - Theft of unattended documentation from a user's workstation.



There are various way to reduce the threat of a data breach, some of which are relatively easy and inexpensive. It's important that management consider the most cost-effective solutions without losing sight of business continuity. The inclusion of new cybersecurity controls should not inhibit the efficiency and productivity of daily business practices. Some of the most cost-effective solutions to implement are:

1. **Educational programs and phishing tests –** Teach employees about the different types of social engineering tactics that will attempt to exploit their naivety on the subject.
2. **Up-to-date antivirus software –** Obtain updates periodically to protect against recently discovered vulnerabilities and other weaknesses that are being exploited.
3. **Current firewalls –** Check with your network protection provider regularly to ensure that your firewall is being improved upon and the most up-to-date version is available.
4. **Continuously monitor and check for network abnormalities** with your current network protection/ firewall software in place; monitor events and activity to see if there has been an increase in unauthorized/ suspicious traffic.
5. **Have a third-party professional service perform a risk assessment** surrounding your business' current environment and infrastructure to identify where your business' vulnerabilities lie. This independent third party may be able to spot weaknesses that have been overlooked by employees who are too close to company operations.
6. **Data mapping exercises –** Before a breach occurs, assess where critical and valuable data resides, flows to and from, and interacts with other systems. This will help you better understand where a malicious attacker could perform the most damage should a breach occur.

There are additional preventative measures that are more robust that you may want to consider, however, they can be more expensive. This includes tasks such as performing penetration tests; deploying intrusion prevention and detection systems; and applying enhanced network monitoring tools to track traffic, timing, frequency, and correlation of data and events.

Corporate culture has gone through a major shift in recent history; a large difference is in the way security surrounds our data. It used to seem as though our data was safe behind a password-protected user ID. Now we see large corporations fall victim to data breaches, jeopardizing the integrity of personal information. It is still commonly seen among small to mid-sized businesses that cybersecurity is not taken seriously. Therefore adequate cyber solutions are often not implemented, seen as cost-effective, or even considered. The size of a business does not guarantee any safeguard from cyber threats, and it is best to keep in mind that no matter the size of your business, you are never too small for a data breach.

Tyler Dwyer is a senior associate in EisnerAmper's PRTS. Questions? Contact him at 732-243-7741 or tyler.dwyer@eisneramper.com.

EISNERAMPER

For more information, please contact us at *eisneramper.com/contact-us*