RSA

WHEN AUTOMATION GOES WRONG

4 CAUTIONARY TALES

AUTOMATION: EVERYBODY'S DOING IT. BUT NOT EVERYBODY'S DOING IT RIGHT.

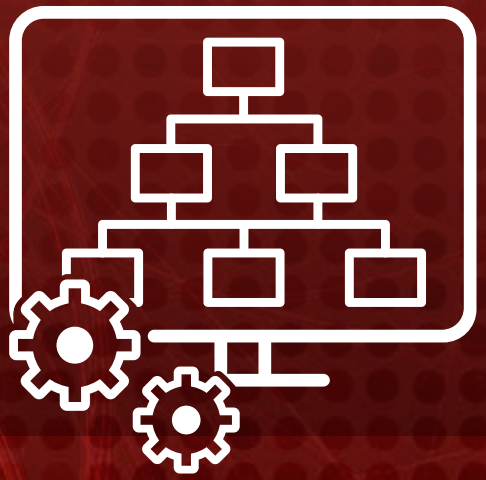
Imagine saving thousands of hours of employee work time, boosting accuracy to near 100% or slashing process times in half. That's the promise of modern process automation technologies, which include robotic process automation (RPA) and cognitive learning, and it's prompting more and more organizations to invest.

In fact, 58% of executives Deloitte surveyed in 2019 said their organizations had started deploying automation technologies.[1]

While automation provides many efficiency and productivity benefits, it also exposes organizations to a host of security, data privacy, resiliency and other operational risks that could have significant financial, regulatory, reputational and even life-threatening consequences.

On the next few pages, we'll take a look at some real-world examples of what can go wrong when automation risk gets out of control—and how it can be managed for a better outcome.

"The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency." BILL GATES



CASE IN POINT #1: THE $7 BILLION BLUNDER

80%

of daily moves in U.S. stocks are machine-led.

Source: CNBC[2]

What happens when automated trading software goes on an unauthorized spending spree? A Wall Street giant nearly goes out of business. In just two decades, the company in question had become one of the largest traders of U.S. equities, with over three billion daily trades worth an estimated $20 billion. But in less than 60 minutes, a bug in its automated high-frequency trading platform almost took down the entire business.

WHAT HAPPENED?

The company had upgraded its automated trading software in response to an SEC decision allowing anonymous transactions. In the process, unfortunately, old test code was inadvertently activated, and one production system was accidentally omitted from the required upgrade. As a result, the company unintentionally bought almost 400 million shares of stock, worth an estimated $7 billion.

Before that fiasco, the company was reaping huge profits from the speed at which its automated platform could execute trades—typically less than 10 milliseconds per trade, or about 40 times faster than the blink of an eye. But when the company couldn't pay for the unintentional trades in the three days allowed by stock exchange rules, it was forced to sell off the stocks at a loss of hundreds of millions of dollars. A year later, it was sold to a rival firm.

Bank on These Best Practices

To err is human, and it may not be possible to avoid the kind of error that led to the unintentional trades described here. But while you can't always prevent human error, you can put technology-based safeguards in place to manage the risk, such as:

- Increased visibility into automated operations
- Stringent testing and monitoring of automated processes
- Coordinated, centralized change management

These and other proactive measures can help ensure that automation continues to improve, rather than impair, operations and outcomes.

CASE IN POINT #2: 270 MINUTES IN DIGITAL DARKNESS

71%

of organizations say the majority of their cloud-resident data is sensitive.

Source: Oracle and KPMG[3]

Two little words no company operating in the cloud wants to hear: major outage. But that's exactly how one cloud service provider characterized an incident that resulted in loss of connectivity and other problems in several areas of the U.S. The issue persisted for three to four hours and likely affected tens of millions of people. As organizations increasingly turn to the cloud to support business-critical applications and services—most of which rely on confidential, sensitive data—the ramifications of a service interruption on this scale can only intensify.

WHAT HAPPENED?

According to the cloud service provider, a bug in its automation software caused a configuration change to be incorrectly propagated to a much larger number of servers than originally intended. People in the affected regions may have experienced increased latency, sporadic errors and service unavailability. Meanwhile, network congestion and outages also hampered the company's ability to troubleshoot the problem.

Ultimately, the cloud service provider resolved the problem relatively quickly, immediately halted use of the software that caused it and announced measures to be taken in the longer term to prevent a recurrence. Still, this leaves the company's customers to wonder if and when another major outage will occur—and what its impact will be on them.

Forecast: Clouds with Good Visibility

In this case, the concern is not just about what the cloud service provider can do to manage the risk of another major outage, but about what the service provider's customers can do to minimize their own risk. An integrated risk management program that includes third-party governance will make it possible to:

- Build a complete inventory of third-party providers, including cloud service providers
- Know which third-party relationships matter most, based on criticality of their services
- Monitor key relationships, related risks and provider performance over time

You can use the information to develop a roadmap for managing risk from multiple providers based on the criticality of services they provide or data stores they support.

CASE IN POINT #3:
2 AIR DISASTERS, 346 CASUALTIES

64%

of workers surveyed report they would trust a robot more than their manager.

Source: Oracle and Future Workplace[4]

A major aircraft manufacturer introduced a new plane into its fleet of popular airliners, with a redesigned cabin and improved aerodynamics that would make it possible for many of the manufacturer's customers to service smaller regional airports for the first time. But what was intended to be a positive business move quickly turned into the company's worst nightmare.

WHAT HAPPENED?

To compensate for a design that included bigger engines, sitting lower to the ground, the manufacturer introduced a new automated maneuvering system that would adjust the trajectory of the aircraft's nose, should the system deem it too high. Unfortunately, failures within the automated systems, combined with inadequate flight crew training, caused the unthinkable to happen.

After making a distress call shortly after takeoff, pilots lost control of the first flight. Minutes later, the brand-new aircraft plummeted into the sea, killing everyone on board. A mere five months later, a second flight found itself in an eerily similar situation, crashing only minutes after leaving the runway. All told, there were two flights lasting a combined 19 minutes—and killing all 346 passengers and crew.

The Crucial Human Element

This story speaks to the importance of having policies and procedures in place to ensure that automated operations are working as intended—and that people are prepared to respond quickly and effectively if not. Key elements include:

- Training and testing to ensure humans can intervene if automations fail
- Regular operator-input requirements, to avoid over-reliance on automation
- Rules and policies that account for variations in underlying technologies

It's always important to proceed with the understanding that automation is not infallible. Doing so could mean the difference between a disaster and a disaster averted.

CASE IN POINT #4: 50,000 FRAUD CASES THAT WEREN'T

65%

of insurance providers in North America and Europe will adopt process automation technology by 2024.

Source: Juniper Research[5]

In every state, thousands of people collect unemployment from the government. But in one state, it was the other way around. A newly automated system for managing unemployment claims flagged 50,000 of them as fraudulent, then demanded the recipients pay back the money they received, with interest. The only problem? The system was wrong.

WHAT HAPPENED?

In an effort to streamline workflows, improve customer service and reduce fraud, a state agency overseeing unemployment benefits instituted a completely automated system for managing unemployment claims. Initial results were an apparent success. The project paid for itself within six months and recouped over $63 million in overpayments and fees.

What the agency didn't know was that much of the money was collected in error, because the automated system incorrectly identified some 50,000 cases as being fraudulent. Eighteen months after the system went live, there were reportedly 30,000 cases awaiting a court trial. (The agency manually reviewed 7,000 of these cases and found that only 8% were actually fraudulent.) And even after several years, there was still at least one class-action lawsuit against the state's software provider making its way through the courts.

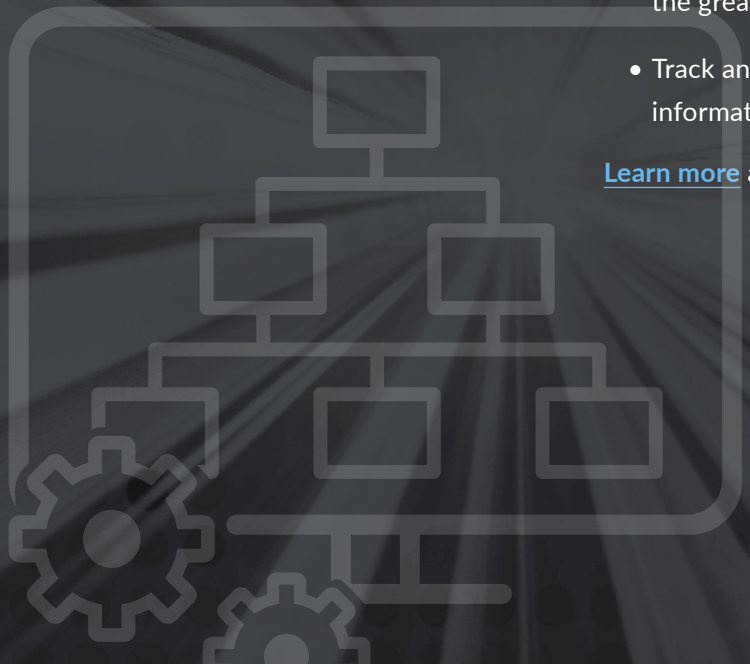
What You Don't Know, You Can't Fix

One of the issues with the automated fraud detection system in this case was that the people overseeing it apparently had little insight into the system and minimal interaction with it—and therefore not much opportunity to detect process problems. This could be addressed by adopting:

- A centralized platform for visibility into risk and improved decision-making
- Automated workflows with real-time analytics and reports
- A mechanism to capture and report insights from business process owners

An integrated risk management approach with deep visibility into automated operations could make it possible to uncover blind spots that might doom an otherwise promising automation initiative.

YOU CAN MANAGE PROCESS AUTOMATION RISK. RSA CAN HELP.



RSA can help you manage process automation risk, protect the integrity and availability of automated processes from cyber attack, and incorporate resiliency, third-party governance and compliance into your business process automation strategy. With RSA, you can:

- Implement a centralized platform that provides enterprise-wide control and visibility into automation risk, drives accountability and improves decision-making
- Assess, treat and monitor automation risk resulting from shifting business needs, system changes and updates, and increasing cybersecurity incidents
- Ensure that users, bots, bot owners and robotic process automation administrators are who they claim to be and have appropriate access
- Gain security visibility and insight across networks, endpoints (including IIoT devices) and users to identify known vulnerabilities and unknown threats
- Translate cyber threats into business terms so that security analysts can focus on the alerts that pose the greatest impact to business-critical automated processes
- Track and manage regulatory obligations related to automated processing of personally identifiable information (PII) and minimize the impact of regulatory change

Learn more about how RSA helps manage process automation risk.

DIGITAL RISK IS EVERYONE'S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA® Business-Driven Security™ solutions provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. With solutions for rapid detection and response, user access control, consumer fraud protection and integrated risk management, RSA customers can thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com

1 Deloitte, **5th Annual Global Robotics Survey,** 2019

2 CNBC, **Sell-offs could be down to machines that control 80% of the US stock market, fund manager says**, Dec 5, 2018

3 Oracle and KPMG, **Cloud Threat Report 2019**

4 Oracle and Future Workplace, **AI@Work Global Study 2019**

5 Juniper Research, **Robotic Process Automation in Telecoms & Insurance 2019-2024**

RSA®