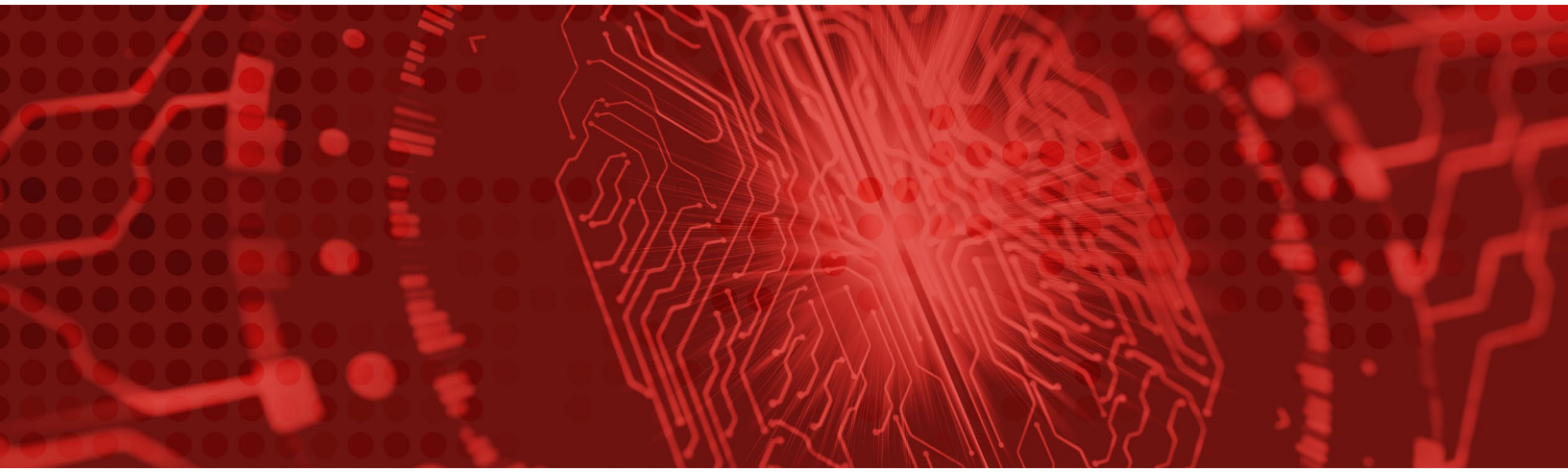
RSA

SOLUTION BRIEF

# MANAGE PROCESS AUTOMATION RISK

## SEIZE THE OPPORTUNITIES. LIMIT THE EXPOSURE.



Imagine saving thousands of hours of employee work time, boosting process 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. As a matter of fact, 58% of executives surveyed by Deloitte in May 2019 said their organizations had started deploying robotic process automation.[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 and reputational consequences, as several organizations have already discovered.

## REAL-WORLD EXAMPLES OF PROCESS AUTOMATION RISK

Consider the financial services company that unintentionally bought $7 billion worth of stocks in one hour due to a flaw in its automated trading software.[2] Then there was the metal producer that got hit by LockerGoga ransomware. The ransomware essentially froze the computers that manage the company's industrial control systems, crippling production and reportedly costing the company $75 million in lost revenue.[3] Last comes the worst-case scenario: the airplane crashes caused by an automated system that malfunctioned, killing hundreds of passengers.[4] These unfortunate examples exemplify process automation risk and its potentially drastic, life-threatening consequences.

## ROOT CAUSES OF PROCESS AUTOMATION RISK

### CAUSE #1: AUTOMATIONS DON'T EASILY CHANGE

Automated processes—whether they're "dumb" or programmed with limited cognitive capacity, whether they run unattended or with some human assistance—rely on a series of preprogrammed instructions and rules to perform mundane tasks and make simple decisions, like adjusting insurance claims or gathering and comparing data from different systems.

This kind of automation lends itself to fairly static processes and activities. The challenge is that most businesses today are anything but static. Evolving business needs, system changes and updates, cybersecurity incidents, and shifting regulatory compliance requirements can wreak havoc on automated processes—yielding unintentional results (as the financial services company learned) or taking services completely offline (as the metal producer experienced).

**Evolving business needs, system changes and updates, cybersecurity incidents, and shifting regulatory compliance requirements can wreak havoc on automated processes—yielding unintentional results or taking services completely offline.**

### CAUSE #2: AUTOMATIONS MOVE FAST AND ARE DEEPLY CONNECTED

One of the key benefits of automation—the speed and efficiency it confers—can at times be a drawback. For example, if there's an error in the instructions that software robots follow or the bots somehow get compromised, they may end up processing large volumes of potentially valuable transactions erroneously before anyone notices. Depending on the work being automated, this could lead a company to misstate its financial results, for example, or make costly order processing mistakes.

What's more, while many bots are trained to interact directly with APIs, the use of APIs to mimic real human users is becoming more popular to streamline complex workflows and automate time-intensive tasks. This creates more internal and external application integrations and cross-solution dependencies, which further amplifies process automation risk.

> *"We're all operating in a connected ecosystem. Risk has been a 'black box' within this model, and the standard assumption is that if each organization manages its own risk, it'll all be OK. But that's not the case. When ecosystems connect and cross, it magnifies the potential risk impact."*
>
> Syed Wajahat Ali
> Senior Director – Security Risk Management
> **du Telecom**

### CAUSE #3: AUTOMATIONS EXPAND THE ATTACK SURFACE

With automation tools readily available to business leaders, IT and third parties, it can be difficult for organizations to identify what non-human workers are being created and where they're being deployed across environments. This new set of "shadow" software provides bad actors with new entry points and vulnerabilities to exploit and share on the dark web.

### CAUSE #4: AUTOMATIONS CONTROL THE MACHINES

The industrial internet of things (IIoT) includes the millions of networked sensors, gauges and actuators that provide reliable electricity, clean water and safe mass transit. It also includes the new generation of industrial robotics that's powering smart factories and ensuring the quality and timely delivery of essential goods and services. Given its role in both critical and commercial infrastructure, IIoT poses the greatest risk of failure.

Unlike traditional IT systems, IIoT devices are typically purpose-designed using legacy or proprietary protocols, with lifespans measured in decades rather than years. They are implemented with a set-it-and-forget-it mindset and upgrading or replacing them can be challenging to nearly impossible. Moreover, thanks to emerging IoT automation platforms, IIoT devices are becoming chained together by rules and instructions—each with its own security flaws—which only serves to increase the attack surface of this highly critical infrastructure.

## BEST PRACTICES FOR MITIGATING PROCESS AUTOMATION RISK

Given the significance of process automation risk, this new non-human workforce of bots, algorithms, artificial intelligence and IIoT requires centralized governance and proper controls. Moreover, organizations must look holistically, through one lens, at the operational and digital risks these technologies create. Operational risk programs built on manual, disconnected or siloed processes will not keep up with the speed at which automated processes need to adapt.

Further, poor access management, privilege abuse, software vulnerabilities, data leakage and denial of service are all very real risks that can impact the integrity and reliability of automated processes and services.

Whether it is a change management issue that disrupts a service offering or a cybersecurity incident that threatens data privacy, organizations require deep visibility into and control over process automation risks in order to effectively identify, assess, treat and monitor automation glitches, changes and attacks.

### BEST PRACTICE #1: USE A COMMON TAXONOMY AND FRAMEWORK

RSA can help you connect fragmented process automation risk strategies to a broader operational risk management strategy using a common platform for managing business and digital risk across your organization. With RSA, you can:

- Establish a comprehensive program to identify, assess, treat and automatically monitor anticipated and unexpected process automation risks.
- Implement a centralized platform that provides enterprise-wide control and visibility into risk, drives accountability, and improves decision-making.
- Streamline process automation risk management by automating workflows and delivering real-time analytics and reports.
- Assess, treat and monitor risk resulting from shifting business needs, system changes and updates, increasing cybersecurity incidents and evolving regulatory compliance requirements.

**Given the significance of process automation risk, this new non-human workforce of bots, algorithms, artificial intelligence and IIoT requires centralized governance and proper controls.**

## BEST PRACTICE #2: PROTECT AUTOMATIONS FROM CYBER ATTACKS

RSA can help you protect the integrity and availability of automated processes from cyber attacks with a comprehensive approach to security monitoring, threat detection and response, and identity and access management. With RSA, you get:

- A high level of confidence that users, bots, bot owners and RPA administrators are who they claim to be.
- Advanced capabilities to govern access for human and non-human workers with role-based access controls. This helps to ensure that only appropriate users have access to bots and automated processes for executing rules, policies and setting tasks.
- Security visibility and insight across networks, endpoints (including IIoT devices) and users to identify known vulnerabilities and unknown threats.
- Cyber threats translated into business terms so that security analysts can focus on the alerts that pose the greatest impact to mission-critical automated processes.

## BEST PRACTICE #3: ACHIEVE CONTINUOUS COMPLIANCE AND RESILIENCY

Finally, RSA can help you extend your business process automation strategy to cover business resiliency, third-party risk, compliance and audit. With RSA, you can:

- Minimize process automation risk by using a common taxonomy and structure for building, testing and implementing business continuity and disaster recovery plans.
- Enable automated processes to naturally adapt to adverse conditions, make midcourse corrections, and avoid the negative impacts of a disruption.
- Assess, treat and monitor business, IT and cybersecurity risk of automated processes associated with third-party relationships.
- Track and manage regulatory obligations related to automated processing of personally identifiable information (PII) and minimize the impact of regulatory change.

## ARE YOUR PROCESSES READY FOR AUTOMATION?

In addition to providing organizations with a comprehensive portfolio of integrated risk management and cybersecurity solutions for managing process automation risk, RSA also provides advisory services designed to help organizations assess their readiness for process automation. RSA can determine the current state of processes, recommend optimizations and provide detailed plans for implementing these changes across integrated risk management tools and technologies. These services can help your organization:

- Enhance process efficiency and improve quality
- Align security and IT services with business priorities
- Establish a basis for greater adaptability
- Define automated process roles and responsibilities
- Minimize process wait states and approvals

**RSA can determine the current state of processes, recommend optimizations and provide detailed plans for implementing these changes across integrated risk management tools and technologies.**

## AUTOMATE WITH CONFIDENCE

With the explosion of RPA, AI and IoT, organizations are justifiably concerned about the impact of these technologies on their computing environments. Continuous system-level changes, the speed and anonymity at which automations run, and an expanding attack surface magnify process automation risk for companies.

Mitigating this risk requires organizations to manage business and digital risk using a common integrated risk management platform, protect the integrity and availability of automated processes from cyber attacks, and incorporate resiliency, third-party governance and compliance into their business process automation strategy.

Only RSA has the people, the technology, the experience, the partnerships and the vision to help organizations effectively manage process automation risk, enabling them to reduce costs, increase productivity, improve accuracy and enhance the customer experience. We're ready to work with you. Contact us now.

## ABOUT RSA

RSA offers mission-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce mission risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change. For more information, go to rsa.com.

1 Richard Horton, et al., "Automation with intelligence: Reimagining the organization in the 'Age of With'," Deloitte, https://www2.deloitte.com/us/en/insights/focus/technology-and-the-future-of-work/intelligent-automation-technologies-strategies.html (September 6, 2019)

2 Henrico Dolfing, "Case Study 4: The $440 Million Software Error…" https://www.henricodolfing.com/2019/06/project-failure-case-study-knight-capital.html (June 5, 2019)

3 Nicole Lindsey, "Reputation Intact Despite Projected Cost of $75 Million for Norsk Hydro Cyber Attack," CPO Magazine, https://www.cpomagazine.com/cyber-security/reputation-intact-despite-projected-cost-of-75-million-for-norsk-hydro-cyber-attack (August 2, 2019)

4 Brian Merchant, "Aviation Experts Have Predicted Automation Will Lead to Disasters…for 15 Years," Gizmodo, https://gizmodo.com/aviation-experts-have-been-warning-us-of-the-dangers-of-1833419813 (March 20, 2019)

RSA