How do you protect the robots from cyber attack?

Securing robotic process automation platforms and enabling cybersecurity through orchestration and cognitive learning.

The better the question. The better the answer. The better the world works.
The cybersecurity robotic Landscape

An increase in cyber attacks, combined with the shift toward automating business processes using robotic process automation (RPA), introduces new risks that must be addressed to secure sensitive data and instill trust in your robotics platforms.

Additionally, the cybersecurity talent gap along with pressures to manage costs makes orchestration and cognitive learning an attractive option for many organizations to improve their security posture more efficiently.
What do we mean when we say robotics?

IT automation (ITA) and business process automation (BPA) have been around for decades – so what’s all this buzz about robotics? We’ve fielded many questions recently as to whether robotics is truly different from traditional ITA/BPA. From our perspective – the answer is a resounding “yes.” While the core objective of automating a process is shared, ITA/BPA is generally built and maintained by a small, technically savvy, centralized team. Robotics inversely places much of the control of automation into the hands of users and less technically savvy individuals. Secondly, ITA/BPA is notorious for taking months and sometimes years to deploy. With robotics, tasks can be automated within weeks due to limited code development and intelligent application screen reading capabilities.

We’re seeing robotics rapidly gaining traction in organizations across many industries and sectors. Business users are employing robotic process automation (RPA) to quickly and easily automate repetitive and time-intensive processes. IT and cybersecurity groups are leveraging the ability of robotics platforms to orchestrate workflows and perform cognitive learning functions. As such, there’s often a bit of confusion about what someone means when they say “robotics.” At EY, we generally see the following three forms of robotics:

1. **Robotic process automation (RPA)** — leverages user-friendly applications to configure software robots that can be quickly trained and deployed to automate manual tasks across various business processes spanning multiple systems. Typical activities considered for RPA include data entry, migrating data across multiple systems, data manipulation, data reconciliation and rule-based decision-making in business processes. These software robots are trained to interact directly with a user interface with no need to develop code to automate individual tasks that assist human staff.

2. **Orchestration (OR)** — often used in IT service management and cybersecurity operations for activities like provisioning and de-provisioning users, ticket management and cybersecurity incident triage. This form of robotics focuses on coding automation actions and actor modules that can be applied to many systems with the goal of streamlining complex workflows and automating time-intensive tasks. It follows a set of predefined rules that describe tasks and makes decisions based on predefined criteria. These solutions interact with application programming interfaces (APIs), databases and back-end servers, often requiring significant code development to set up required modules with the ability to leverage these modules at a later time with less need for code development skills.

3. **Cognitive learning (CL)** — this form of robotics moves beyond rule-based decision-making for processing both structured and unstructured data to incorporate machine learning and artificial intelligence through the application of advanced algorithms and analytics. Cognitive learning aims to think and act the same way as humans do in order to perform complex tasks without human interaction. As such, this requires extensive programming and modelling of machine and self learning algorithms.

<table>
<thead>
<tr>
<th>Key attribute of robotics</th>
<th>RPA</th>
<th>OR</th>
<th>CL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interacts with user interface</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intelligent screen scraping</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trained by business users</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Rule-based decision-making</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trained by IT admin and IT security analysts</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interacts with APIs and databases directly</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Requires significant code development</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Trained by skilled programmers/developers</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Artificial intelligence/machine learning</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

How do you protect the robots from cyber attack?
In the current business environment with a pressing need to digitize, robotics is a critical component of an enterprise’s digital strategy. As robotics is applied to various facets of an enterprise, a robotics program should both address cyber risk by securing robotics platforms as well as leveraging robotics to enable the execution of more effective and efficient cyber operations. We believe the six cyber domains outlined below play the most critical roles in robotics. Through the remainder of this document, these six domains will serve as our lens to view robotics security.

**A cybersecurity framework for robotics**

**Digital identity and access management**
- Access fulfillment, provision/de-provisioning, access certification, access analytics, privileged access management

**Data identification and protection**
- Data classification, data protection, data usage monitoring and data privacy

**Resilience**
- Protecting, detecting and reacting to cybersecurity threats via business risk, ecosystem management, critical asset defense, board leadership and cybersecurity readiness

**Governance**
- Strategy, policies and standards, metrics and reporting, ongoing

**Security operations**
- Cybersecurity threat detection response (TDR), threat exposure management (TEM)

**Software and product security**
- Secure software development, threat modeling, static/dynamic code scanning, vulnerability identification

How do you protect the robots from cyber attack?
How do you protect the robots from cyber attack?

Securing robotic process automation platforms and enabling security through orchestration and cognitive learning.
What are the cyber risks associated with RPA?

RPA introduces a new attack surface that can be leveraged to disclose, steal, destroy or modify sensitive data and/or high-value information, access unauthorized applications and systems, and exploit vulnerabilities to gain further access to an organization. One of the most popular questions we hear today is, “Which cyber risks should I be concerned about for my robotics capabilities?” In this section, we focus on RPA cyber risks, leaving specific considerations about cognitive learning to be covered at another time.

At EY, we believe organizations must build trust in their RPA platforms to address many forms of risk, including cyber risk. Some detailed examples of robotics-related cyber risks organizations should consider as they work to secure their robotics implementations include:

<table>
<thead>
<tr>
<th>Cyber risk</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abuse of privileged access</td>
<td>▶ An attacker compromises a highly privileged robotic user account used by some bots to gain access to sensitive data and move laterally within a network.</td>
</tr>
<tr>
<td></td>
<td>▶ A malicious insider trains a bot to destroy high-value data, interrupting key business processes, such as customers generating orders.</td>
</tr>
<tr>
<td>Disclosure of sensitive data</td>
<td>▶ A bot creator mistakenly trains a bot to upload credit card information to a database accessible via the web.</td>
</tr>
<tr>
<td></td>
<td>▶ A bot creator leverages a generic account to steal sensitive intellectual property, leaving it difficult, if not impossible, to identify true source of the leak.</td>
</tr>
<tr>
<td>Security vulnerabilities</td>
<td>▶ A vulnerability exists in robotics software that provides attackers remote access to an organization’s network.</td>
</tr>
<tr>
<td></td>
<td>▶ A bot creator trains a bot to handle sensitive customer data but does not secure/encrypt the transmission of that data to/from the cloud.</td>
</tr>
<tr>
<td>Denial of service</td>
<td>▶ A bot is scheduled to execute in rapid sequence resulting in exhausting all available system resources and halting all bot activities.</td>
</tr>
<tr>
<td></td>
<td>▶ Bot controller is disrupted due to unplanned network, service or system outage resulting in lost productivity, not easily replaced with human labor.</td>
</tr>
</tbody>
</table>
How can I secure my RPA ecosystem?

When it comes to securing RPA implementations, an organization must consider the technical, process and human elements of the entire robotics ecosystem. A secure design should include the entire product life cycle from requirements, selection, architecture, implementation and ongoing operations. To build trust within a robotics platform, we believe your approach should provide the following:

1. Integrity: Can I trust that the data and results I get from my bots has not been modified or altered?
2. Traceability: Am I able to monitor and track bot activities to identify the misuse of robotics affecting confidentiality, integrity or availability of other systems/data?
3. Confidentiality: Can I protect sensitive data from being purposely or accidentally disclosed by bot creators and bot runners?
4. Control: Am I controlling access and protecting privileged accounts leveraged by the robotics system and users?

Leveraging the cybersecurity framework for robotics outlined previously, we’d like to discuss security control considerations for each cyber domain.
## How can I secure my RPA ecosystem? (continued)

<table>
<thead>
<tr>
<th>Control</th>
<th>Robotic details</th>
</tr>
</thead>
</table>
| Governance                   | ▶ Establish a governance framework with roles and responsibilities for securing robotics  
▶ Build strategy and security requirements for RPA within policies and monitor compliance with security policies related to RPA  
▶ Manage RPA risks identified through a formal risk management program and increase awareness among bot creators and business users around the risks of RPA |
| Software and product security| ▶ Perform security architecture risk analysis of chosen RPA solutions, including bot creation, control and running. Identify security architecture flaws in underlying product for connections across various environments, usage of virtualization methodologies, and authorization flaws  
▶ Conduct secure design review, including data flow analysis to verify that controls around security are integrated into the bot authentication, authorization and input validation  
▶ Integrate security scanning tools as part of the bot creation process to scan code created in the back end for security vulnerabilities  
▶ Scan bot created for security vulnerabilities using dynamic testing or security fuzzing technology to determine security flaws  
▶ Ensure schema for bot deployment has security considerations in place |
| Digital identity and access  | ▶ Improve auditability (every step could be logged) and control over error-prone manual activities that elevate risk and noncompliance  
▶ Manage user access privileges/segregation of duties risk; for example, use of a specialized security matrix authorizes bots to only perform the tasks assigned to them  
▶ Implement security controls to protect credentials during robotic session run-time; for example, use of single sign-on (SSO) with lightweight directory access protocol (LDAP) supports secured logon to RPA interface  
▶ Enforce passwords consistently across robotic sessions and centralize robotic identity and access management process; leverage encrypted credential managers to prevent leakage of credentials |
| Data identification and protection | ▶ Conduct compliance assessment to data regulations for use of robotics and automation  
▶ Monitoring of sensitive data processed by robotics/automation to verify compliance with usage policies  
▶ Integrity checking of robotics and automation code |
| Security operations          | ▶ Gather log data from controller and bot runners to provide an audit trail of activities, monitoring for abnormal spikes in activity, access of systems and use of privileged accounts  
▶ Conduct vulnerability scanning of your robotics platform and execute threat modelling exercises of robotics sessions to determine technical weaknesses or process gaps |
How do you protect the robots from cyber attack?

Securing robotic process automation platforms and enabling cybersecurity through OS threat and cognitive learning.

Leveraging robotics for cybersecurity
How can robotic automation and orchestration improve your security organization?

Many chief information officers (CIOs), chief information security officers (CISOs) and chief digital officers (CDOs) are challenged by tens and often hundreds of legacy technologies and applications that do not work well with one another. This leaves their people manually gathering data from multiple systems, copying information from one system to another and switching between far too many applications to complete a single task. To combat this, a new category of capabilities is becoming more popular in the cybersecurity domain. Organizations are using these forms of robotics to:

► Reduce time to detect and respond to incidents, helping minimize risk exposure to an attack
► Close the talent gap by automating resource-intensive tasks, helping organizations to manage operating expenses
► Minimize employee turnover due to lack of challenge or career progression by allowing employees to focus on higher value tasks
► Automatically deploy security controls when vulnerabilities or compliance exceptions are discovered resulting in a reduced attack surface
► Make intelligent decisions quickly, resulting in high-quality and consistent outcomes

EY thinks robotics will help fill the anticipated talent shortage of 1.5m cybersecurity professionals by 2019.¹

EY believes robotics can help significantly reduce the average time to detect from the current 205 days² to weeks or even days.

74% of security professionals are concerned about insider threats.³ EY believes robotics can help by reducing employee exposure to sensitive data.

¹ Source: (ISC).
² Source: Gartner.
³ Source: SANS
# Illustrative use cases to apply robotics in cybersecurity

We previously discussed the potential security concerns associated with robotics; however, there are also several opportunities to leverage robotics to enhance your digital strategy, as well as improve security operations. We will use the cybersecurity framework for robotics, introduced previously on page 2, to illustrate potential beneficial use cases.

<table>
<thead>
<tr>
<th>Cybersecurity domain</th>
<th>Illustrative use case</th>
</tr>
</thead>
</table>
| Governance           | **Security program governance**  
Robotics can improve security reporting quality, timeliness and throughput. For example, automated, periodic security posture testing can be fed to a robotics-driven, comprehensive reporting process, providing managers dashboards and highlighted areas of concern (outside of management-established tolerances/metrics).  

**Security controls tracking**  
Robotics can help drive automated testing within the information security space. For example, within configuration, robotics could enable faster and more efficient compliance testing to policy for security settings on servers, firewalls, routers and applications. Tests could be conducted on a periodic basis and fed into automated reporting for dashboarding, etc. |
| Software and product security | **Application inventory tracking**  
Robotics can be leveraged to automate the discovery and inventory applications in the enterprise. Once discovered, cognitive learning can be used to automate the risk classification of the application based on data and controls discovered. Additionally, bots can be deployed to continuously discover and update the inventory and associated controls.  

**Secure development gates**  
Cognitive learning can be used to perform gate checks for security activities in the software development life cycle (SDLC). Bots can collect information from each project management tool or through automated systems to identify when a code base is moving to the next phase of the SDLC. Rules can be set and fed into automated reporting for dashboarding, etc., to understand if the security debt on an application should be remediated.  

**Security validation and remediation**  
Robotics can be used to gather automated information regarding the URLs and code that need to be tested to enable efficient analysis of the applications for vulnerabilities. Bots can enable efficient scaling of multiple applications at the same time and complete Tier 1 triage of the vulnerabilities discovered. Results of the tests can be integrated with existing developer platforms for remediation through cognitive learning bots as well. |

---

How do you protect the robots from cyber attack?
## Illustrative use cases to apply robotics in cybersecurity (continued)

<table>
<thead>
<tr>
<th>Cybersecurity domain</th>
<th>Illustrative use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital identity and access</td>
<td><strong>Access fulfilment</strong>&lt;br&gt;Robotics can help reduce dependency on large help desk and operations teams by automating the majority of provisioning/de-provisioning tasks. It may deliver up to 8x improvement in automated request fulfillment time frames compared to manual processing.</td>
</tr>
<tr>
<td></td>
<td><strong>Access certification</strong>&lt;br&gt;BOTs can be trained to achieve up to 45% operational and cost efficiency gains by automating the manual precertification data validation checks, certification configuration management, manual campaign checks during access certifications/reviews, post certification reconciliation and reporting.</td>
</tr>
<tr>
<td></td>
<td><strong>Manual access appropriateness check and automated alert notifications</strong>&lt;br&gt;Robotics can help improve the efficiency and quality of access data validation, allowing managers to focus on higher-risk access concerns during the review process. It can also be trained to compose and send confirmation notifications to users if any anomalies are detected while performing data validations.</td>
</tr>
<tr>
<td>Data identification and protection</td>
<td><strong>Data discovery, classification and remediation</strong>&lt;br&gt;Robotics can be leveraged to automate the discovery and inventory of sensitive data. Once discovered, cognitive learning can be used to automate the classification of sensitive data. Additionally, bots can be deployed to discover, validate and remove sensitive data stored in unauthorized locations.</td>
</tr>
<tr>
<td></td>
<td><strong>Data loss detection and remediation</strong>&lt;br&gt;Cognitive learning can be applied to improve accuracy of insider threat and data loss monitoring. Once issues are discovered through data loss monitoring, data security controls can be automatically deployed to remediate offending systems and prevent future issues.</td>
</tr>
<tr>
<td>Security operations</td>
<td><strong>Threat detection and response</strong>&lt;br&gt;Robotics can be used to gather relevant threat intelligence and technical data to enable quick and efficient analysis of malware and threat alerts. Once gathered, robotics logic can help automate the Tier 1 triage process to make decisions on when and how to respond. Additionally, automated actions can be taken to coordinate remediation of incidents.</td>
</tr>
<tr>
<td></td>
<td><strong>Threat exposure and vulnerability management</strong>&lt;br&gt;Robotics can improve the efficiency and quality of the threat and vulnerability program, helping to understand enterprise vulnerabilities and prioritizing remediation activities. It can then be leveraged to automatically notify system and application administrators of the remediation activities and conduct validation to track compliance.</td>
</tr>
</tbody>
</table>
How do you protect the robots from cyber attack?

**Access fulfilment use case for robotic process automation**

Robots can be deployed to gather the manual work item information from the Identity Access Management (IAM) solution and automate the execution of the access fulfilment tasks on the end systems.

### Manual

<table>
<thead>
<tr>
<th>User</th>
<th>Help desk</th>
<th>Approval team</th>
<th>Admin team</th>
</tr>
</thead>
</table>

### Access

- **DB team**
- **AD team**
- **App team**

### Fulfillment

- Database
- Directory server
- Legacy server

### Robotic

<table>
<thead>
<tr>
<th>User</th>
<th>Help desk</th>
<th>Approval team</th>
<th>Admin team</th>
</tr>
</thead>
</table>

### Access

- **DB team**
- **AD team**
- **App team**

### Fulfillment

- Database
- Directory server
- Legacy server

**Benefits:**
- **A 6x–8x improvement** by taking a 6–8 minute manual process and reducing to ~1 minute
- **Robot can provide 24/7 coverage**, handle tasks by itself
- **Includes exception handling logic** for business exceptions, system exceptions and data validations
- **Solution has the ability to review audit logs, schedule and handle tasks** by itself
- **Multiple robots can be deployed** to have parallel activity based on the transaction volumes

---

How do you protect the robots from cyber attack?
### Phishing use case for robotic orchestration

Phishing attacks are one of the most common threats facing organizations today. Properly analyzing and responding to a phishing email can be a time-intensive process for just a single email. This makes the phishing response process an excellent candidate for automation.

Through automation of virtually the entire data gathering process, most of the analysis and some of the remediation tasks, organizations can address more alerts more effectively, helping improve risk management and reduce attack surface.

<table>
<thead>
<tr>
<th>Activities</th>
<th>Data gathering</th>
<th>Analysis</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extract indicators (URLs/IPs) from message</td>
<td>► Inspect message headers&lt;/br&gt;► Cross-reference URLs/domain/IP address with threat intelligence</td>
<td>► Read for suspicious grammar&lt;/br&gt;► Scan attachment for malware&lt;/br&gt;► Extract malware indicators: IP/URL/Hash/process&lt;/br&gt;► Query SIEM&lt;/br&gt;► Pivot to point solutions&lt;/br&gt;► Validate authentication logs</td>
<td>► Run antivirus scan&lt;/br&gt;► Execute response procedures or preloads response steps in point solutions&lt;/br&gt;► Update firewall/spam filter&lt;/br&gt;► Disable user accounts&lt;/br&gt;► Purge from email server&lt;/br&gt;► Update ticketing system&lt;/br&gt;► Notify affected parties</td>
</tr>
<tr>
<td>Compare threat intel sources</td>
<td>► Generate reports&lt;/br&gt;► Create ticket with relevant information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generate reports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create ticket with relevant information</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Time (pre-automation) | 10 mins | 10 mins | 20 mins |
| Time (post-automation) | ~4 mins | ~4 mins | ~4 mins |

50% to 75% reduction in time to detect and respond to a phishing attack
Would you like to know more?

Robots are here. Are you prepared?
Robotic process automation and the evolving risk landscape

Robotic process automation: development lifecycle and processing risk and control considerations

Three lines of defense in robotic process automation.

Robotic process automation and the third line of defense: an internal audit perspective

How do you protect the robots from cyber attack?
How do you protect the robots from cyber attack?
How do you protect the robots from cyber attack?

Securing robotic process automation platforms and enabling cybersecurity through orchestration and cognitive learning.

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY’s Advisory Services
EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions, create innovative answers and realize long-lasting results.

The better the question. The better the answer. The better the world works.