ANOMALIX

ANOMALIX
WHITE PAPER
Securing Robotics

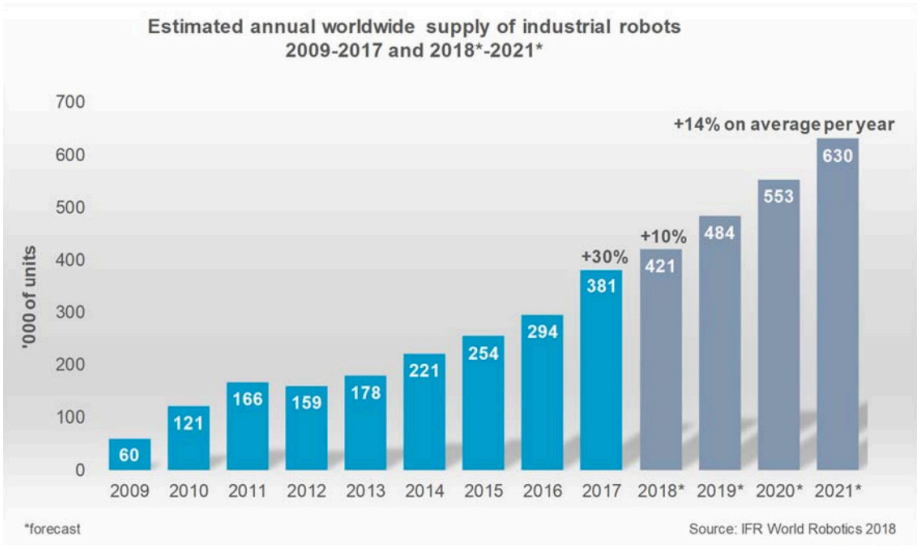
Securing Robotics

Humans have always held a fascination with robots. Robotics are the unusual fusion of art, technology and engineering. From the initial design of mechanical devices to perform tasks in Ancient Egypt and Greece to the 1950s and 60s versions of what we now call a robot, we have been in an eternal search to create technologies to assist us in life. We have surrounded ourselves with robots in movies as well as space exploration, and with each step, we move closer to the visions of both science fiction and fact. Even the ultimate Renaissance man, Leonardo da Vinci, dreamed of functioning robots.

We have surpassed Isaac Asimov's insightful idea of robotics as helpful tools and have now entered the next stage, where convenience and cost-effective aspect of robotics is the next wave of technology for Industry 4.0. Robotics are part of many verticals, from manufacturing and healthcare to human-like robots, and in the world of industrial internet of things (IoT), security is a priority. We are currently facing the challenge of trying to keep up with the fast pace of the future while protecting the technologies that we are creating. Cybercriminals have taken keen notice of this landscape, and even Asimov may not have anticipated the place that we find ourselves today. Traditional methods used to combat cybercrime are not effective. If steps aren't taken, the costs will spiral out of control. The Center for Strategic and International Studies (CSIS) estimates that the global cost for cybercrime last year may be as much as $600 billion.

Robotics are going to continue to be part of our lives and businesses. It's time to re-evaluate how we perceive robotics and deal with their security.

Robotic Process Automation (RPA) Industries



According to the International Federation of Robotics (IFR): Industrial sales of robots are increasing almost exponentially. 2017 saw 387,000 units sold, achieving a 31%increase over 2016. By the year 2021 sales are expected to reach 630,000 units.

There are two scenarios that surround the topic of industries using robotics: the top industries that are using them now and the sectors that are ramping up use for the future. Current high-volume use includes manufacturing, healthcare, and agriculture. In the near future, we will see more robotics in elderly care, construction, retail, automotive, finance, and driverless vehicles. Robotics will be playing even more of a critical role in technology.

The Game Has Changed for Industry 4.0

Companies are launching a fusion of robotics, AI, and automation, in combination with a savvy workforce. However, the concept of security that has historically been used has been mainly a hit or miss strategy to thwart the next attack method. IT departments are scrambling to try to ensure that everything is secure and tied down, and cybercriminals seem to circumvent each action by finding loopholes and new attack approaches. Where once the criminals were expected to make hacking attempts via a system's backdoor, they now waltz through the front door, and in some cases, are invited in. A majority of employees use work technologies to surf the web and they get trapped in phishing expeditions that will access their user account or lead them to a website that downloads malware or a virus. Adding insult to injury, cyber criminals have also become so successful that their organizations emulate the sophistication of true technology companies.

Internet Dangers and System Breaches

One of the most popular forms of front door system breach has been through the use of ransomware. An infected file is sent to a staffer as an attachment, and when opened, the malware infiltrates an entire network and holds it ransom for payment. In the last few years, the healthcare industry experienced numerous and costly attacks via ransomware, and most were successful through simple emails. In this form of attack, every aspect of a network is compromised, including any robotic systems. However, data can be a lot more valuable, and we saw the breach of sensitive materials from over 100 manufacturing companies that had data exposed on a server belonging to Level One Robotics that was publicly exposed. The companies included Chrysler, Fiat, Ford, GM, Tesla, Toyota, Thyssen Krupp, and VW. The problem occurred when the rsync server lacked restrictions so that the rsync port was accessible for data downloads. It can be clearly stated that anything that has a connection to the internet is vulnerable.

Future Outlook for Robotics

As the use of robotics continues to escalate, detecting security risks has become paramount. Identity access management is an integral part of protecting proprietary data and technology, and cybersecurity has become a part of the cost of doing business. Leading trends that include mobile robots and human-robot collaboration means that there will be increased autonomy, and intelligence will move beyond networks to individual brains. With AI-enabled robots, there is heightened concern that their software will be the vulnerable point for cyberattacks. The future of robotics will contain each of these elements, and we will see a convergence of OT (operational technology) and IT (information technology) to a point where they may be indistinguishable.

Vision
To successfully secure robotics in Industry 4.0 leaders should:

- Establish Visibility into all access points to determine who and what has access
- Develop a defined roadmap for implementation, detection, reaction, and defense as part of the ecosystem management
- Create a digital pathway with access certification and privileged access management
- Incorporate a standard for both human and non-human credentials
- Develop a Robotic Process Automation (RPA) Tool Strategy
- Create a Governance Framework for current and ongoing robotic implementation

Leaders know that all connected robots are a risk without proper security policies and governance and must incorporate the proper policies and tools to secure the organization.

Where to Begin?
Security starts with visibility. Ensure that everyone involved in positions that interact with the technologies have a clear understanding of what robotics are connected, the location of connectivity, who has access, and all data in/out touch points. This must cascade to every kind of connected device, resource, and access throughout your organization. In the Industry 4.0 universe, every avenue needs to be examined for your protection. You will need to establish security teams and protocols and set new policies into place that will require compliance.

Conclusion

Robot security is more vital than ever. As robotics continue to get implemented into current and new industries, it becomes necessary to analyze every aspect of your robotics technology. Anomalix can help solve your Industry 4.0 robotic challenges by identifying problems and assist in securing against potential threats.

Anomalix works with your organization to build a custom solution that is unique to your business needs by:

- Determining all levels of system access and data transferal so that we can recommend changes to tighten security.
- Our Subject Matter Experts (SME)assist with your strategy by defining your business initiatives and coordinate with your team to determine the best methods for the integration of your robotic devices into your security infrastructure.
- Working with your current condition and then craft a roadmap to guide you for future changes and the adoption of new devices and technologies.

What are the Results?
A well-orchestrated plan requires an understanding of current security requirements and a continuing strategy to address the changing landscape of the fu-

ture. By beginning with visibility and developing an ongoing strategy, organizations can ensure the security of robotics.

Visibility into all Access Points
Determining visibility allows an organization to understand who and what has access. Visibility delivers details on all connectivity pathways, data transmissions, and individuals with all forms of access. By understanding every access point, security teams can identify areas that need improvement and support.

A Defined Roadmap for Implementation
Developing an inclusive, proactive strategy that incorporates stakeholders is necessary to have a secure robotics program. Communication with teams enables security leaders to build a roadmap for implementation and governance. Incorporating your robot vendor into these initiatives can lead to the development of customized solutions that fit your environment. By having a road map, robots can be incorporated into your ongoing security strategy. If the robotics program is in its infancy, developing an inclusive program will help build a strong foundation for security.

Access certification and Privileged Access Management
Incorporating access certification, privileged access management, and second level security access must be part of your digital pathway. The security requirements and strategies that are needed should be combined with those who hold responsible roles in monitoring compliance.

Differentiated Human and Robot Credentials
In order to secure robotics, it should be required to use unique human credentials that are differentiated from those assigned to bots. In addition, it must be combined with consistent credential changes. This action will assist in maintaining security at the known access points while exposing any breaks in duty segregation that could lead to vulnerabilities.

Implementing an RPA Life Cycle Strategy
Using the power of your RPA, your technology team is enabled to formulate analysis, audit trails, alerts for suspicious activities, compliance conditions, misuse, and weaknesses.

Implementing an RPA Life Cycle is an integral part of your strategy that goes beyond just day to day operations. Instituting an analysis phase that moves towards development, testing, deployment, and maintenance. Crafting a well-orchestrated life cycle will also include the various nuances of change that occur over time. Each phase will evolve as new devices and technologies are incorporated.

A Governance Framework for Current and New Robot Implementation
Developing and implementing a governance framework is essential to an ongoing robotic risk management program. Maintaining constituency to ensure all touch points, vendors, and products comply with your security requirements.

By learning the current and evolving conditions of robotics in Industry 4.0 from this research, Security leaders and stakeholders can expand their knowledge of the new conditions and incorporate robots into security programs.

Third-Party Identity Management in a Decentralized World

Contact: info@anomalix.com

Headquarters
1180 Town Center Dr.
Suite 100
Las Vegas, NV 89144