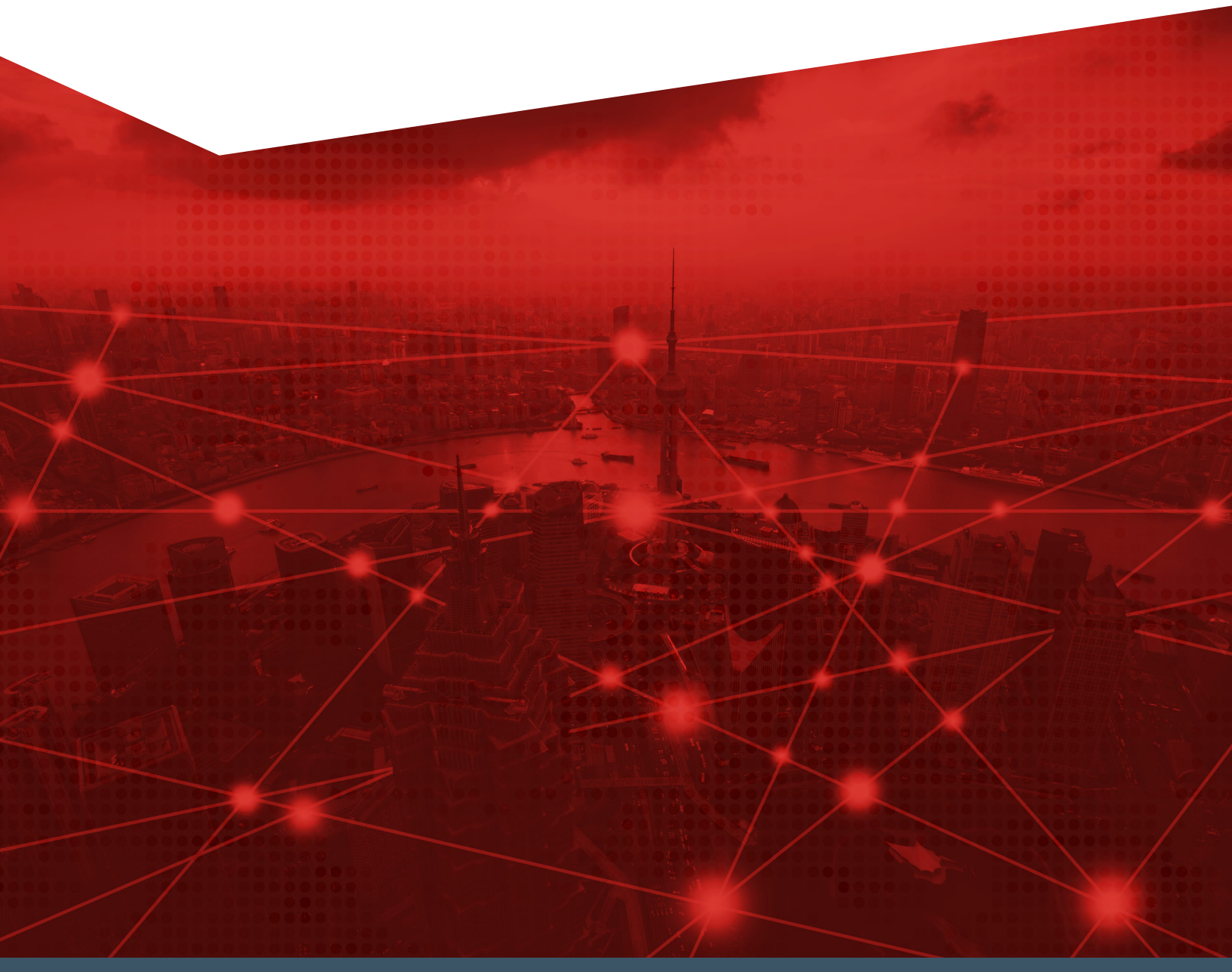
RSA

WHITE PAPER

DIGITAL RISK IN THE INTERNET OF THINGS



DIGITAL RISK IN THE IoT

The Internet of Things (IoT) is a core component of digital transformation, along with cloud, mobile, automation and analytics. The explosion of IoT technology is enabling whole, new categories of value, integrating real-world data and processes into standard computing and automation toolsets.

But as with all digital transformation, the benefits come with some unique risks. These billions of diverse devices, ranging from the largest-scale industrial systems to your fitness tracker, impact key areas including cybersecurity, third-party risk, compliance, data governance and privacy, automation, and business resiliency.

Here are some of the primary challenges to securing IoT digital risks:

- Scale—In a November 2018 press release, "Gartner forecasts that 14.2 billion connected things will be in use in 2019, and that the total will reach 25 billion by 2021 … By 2023, the average CIO will be responsible for more than three times as many endpoints, producing immense volume of data."

  Of course, this explosion of devices creates an explosion of data. Storage systems must be designed to accommodate the volume produced by these devices. And security and privacy controls need to be in place to protect all that data, much of it personal.

- Variety—Complicating the scale issue is the sheer variety of devices in a typical organization. Once mainly the province of operational technology (OT) such as power grids, manufacturing systems and building controls, IoT now includes a dizzying array of sensors, cameras, thermostats, trackers and other networked devices. Consumer devices such as wearables and home assistants (e.g., Amazon Alexa) create a rich platform for new services. Critical industrial control systems (ICS) deliver power, water and transportation services as well as manufacturing processes like robotics. Large-scale government projects like the Smart Cities Initiative break new ground in delivering services and improving quality of life for residents.

  Unlike traditional IT systems, IoT systems are typically purpose-designed, with lifespans often measured in decades, not years. Upgrading or replacing devices in place is challenging or impossible—due to both physical location and memory/processing limitations. Data formats vary widely. And some systems are designed as siloed solutions that were never meant to integrate with modern management and security methods.

- Standards—Industry-led standards are essential for development and growth of an interoperable and secure IoT ecosystem. As IoT matures, there needs to be a consolidation among the competing initiatives and better coordination across the complementary efforts in order to ensure the desired interoperability, security and manageability of IoT solutions.

- Regulations—Risk management typically requires conformance with government or industry regulations. For ICS, there is NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security. But security regulations are quickly being developed for all IoT systems.

These billions of diverse devices, ranging from the largest-scale industrial systems to your fitness tracker, impact key areas including cybersecurity, third-party risk, compliance, data governance and privacy, automation, and business resiliency.

- Data—Often, sensitive data such as production information or customer records are processed via IoT devices. This data is subject to the same privacy controls as other data but can be overlooked or even completely isolated from control systems, opening up a large risk for organizations.
- Human factors—IoT risks mirror, or even amplify, the human factors in other digital risk areas. A 2017 survey of 1,845 IT and business decision-makers by Cisco across a range of industries shows that 60 percent of IoT initiatives stall at the proof of concept (POC) stage and only 26 percent of companies have had an IoT initiative that they considered a complete success.

RSA helps customers manage all these digital risks driven by IoT deployments. RSA products and services address IoT risks across several critical areas including Integrated Risk Management (IRM) with RSA Archer®, security monitoring with RSA NetWitness® and RSA IoT Security Monitor, and identity with RSA SecurID®. Additionally, the Dell Technologies IoT ecosystem, including the open standard EdgeX Foundry, provides a compelling RTM where RSA provides the risk and security componentry of a comprehensive IoT management solution.

The proliferation of IoT endpoints creates a huge strain on operational security:

- The massive scale of IoT deployments demands solutions that are manageable at scale. This includes securing the connected "things" throughout their lifecycle, from on-boarding and provisioning to operations, monitoring, maintenance and update.
- Many brownfield deployments consist of devices with embedded controller and logic, which were built using legacy protocols for connectivity within a private/local network (e.g., a shop floor or a building). With IoT, this connectivity is extended to apps and services in the cloud or in a back-end data center. It is not always possible to replace or upgrade these devices, especially in cases where such devices are expected to stay in service for many more years.
- Many IoT devices lack the minimum compute and power required for performing security functions that are common for a typical IT device.
- Depending on the use case, the IoT devices may be deployed in the field and in potentially hostile locations with no physical security guarantees (e.g., an unmanned wind turbine or traffic sensors in a smart city use case). In such scenarios, the IoT devices require additional protection measures against physical attacks such as manipulating, replacing or spoofing devices.

The massive scale of IoT deployments demands solutions that are manageable at scale. This includes securing the connected "things" throughout their lifecycle, from on-boarding and provisioning to operations, monitoring, maintenance and update.

Addressing these challenges is a growing priority for organizations around the globe, often driven by emerging standards and regulations. Some examples of standards in use or in development include:

- DDS—The Data Distribution Service (DDS) is a middleware protocol and API standard from the Object Management Group (OMG) for machine-to-machine communication.
- EdgeX Foundry—EdgeX Foundry is a vendor-neutral open-source project building a common open framework for IoT edge computing. (Dell Technologies seeded this project with FUSE source codebase

under Apache 2.0.)

- FIDO Alliance—FIDO Alliance develops specifications and certifies interoperable products for stronger authentication.
- IEC 62443—This is a suite of standards and technical reports that define procedures for implementing secure Industrial Automation and Control Systems (IACS).
- IETF ACE—Authentication and Authorization for Constrained Environments (ACE) is an IETF standard targeting the low-power, low-compute IoT devices.
- IETF CoAP—The Constrained Application Protocol (CoAP) is an IETF standard that defines a specialized web transfer protocol for use with constrained nodes and constrained networks (e.g., low-power, lossy).
- IIC—The Industrial Internet Consortium (IIC) sets the architectural framework and direction for the Industrial internet using open standards.
- MQTT—Message Queue Telemetry Transport (MQTT) is a lightweight publish/subscribe messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks.
- OPC UA—The OPC Unified Architecture (OPC UA) is a broadly adopted industrial automation standard for secure and reliable exchange of data in mission-critical industrial applications.
- OpenFog—The OpenFog Consortium is formed to accelerate the adoption of fog computing, a computing paradigm that attempts to address the bandwidth, communication and latency challenges associated with IoT.

Regulations are quickly emerging as well. From Security Boulevard:

- The United Kingdom recently announced intentions to introduce new laws requiring security to be built into IoT devices. This adds to the government's 2018 release of the world's first IoT code of practice. This includes guidelines for manufacturers, such as no default passwords, securing credential storage and ensuring software integrity.
- The U.S. Congress is waiting to vote on the IoT Cybersecurity Improvement Act of 2019, which would allow the standards body, NIST, to draw up IoT regulations.
- The Japanese government will begin enforcing IoT standards next year. They are currently working out what those standards might include, such as mandatory device identity to prevent unauthorized access and control for over-the-air updates.
- Recently, ETSI came up with a new "global standard" for IoT, which builds on the U.K. government's IoT code of practice.

IoT SECURITY IS NOT JUST ONE THING

Based on our research and discussions with customers and analysts, RSA has identified six areas that are critical for IoT end-to-end security (Figure 1).

These six areas are:

FIGURE 1: Critical IoT Security Areas

- **Discovery, Identification & Classification**—The discovery process detects the existence of an endpoint at a certain IP address. The identification process then takes this to the next level by detecting the specific information about the device; for example, detecting that a device is a motor from a certain manufacturer. Additional information such as model number, serial number and firmware version number may also be captured. This metadata is correlated with additional information such as known vulnerabilities, operational strengths and weaknesses, and common misuse and misconfiguration scenarios about the device. This deep classification creates additional granularity in tracking and reporting.
- **Risk Management**—Once IoT devices are identified, they must be assessed continuously for associated risk. The risk profile of an IoT deployment changes over time, affected by activities such as adding and removing devices to/from the network, changes to access policies, discovery of new vulnerabilities, and the firmware/software updates applied to devices. Third-party risk arises, associated with the exchange of IoT data between the enterprise and external service providers. And as digital transformation continues and IoT technology matures, there will be an increasing number of regulations and guidelines for enterprises to track and comply with, such as FDA guidelines for cybersecurity of connected medical devices.
- **Authentication & Access**—Enforcing authentication and access policies ensures operational integrity of the connected environment. This includes protecting access to and from the device. The strengths and weaknesses of access policies should be dynamically reflected in the continuous risk assessment of the overall environment.
- **Monitoring & Threat Detection**—The massive scale of IoT deployments and prevalence of low-power devices creates security and risk challenges but offers one advantage: an abundance of IoT operational data and use data. Analytics can profile devices, baseline the normal behavior, and detect and alert on anomalous activities and compromised devices. Leveraging machine learning and with no requirement to changing IoT devices, these techniques can secure large deployments of sensors and actuators.

- **Data Protection**—The data collected from connected devices is critical to the success of any IoT project. The integrity of IoT data is fundamental to arriving at the desired business insight, reliable operational decisions or sound security analysis. The protection of the data at rest, in transit, or in process is critically important in today's privacy-focused landscape.
- **Secure Device Management**—It is essential to have a secure solution for device management in an IoT deployment. As a minimum, this includes secure remote maintenance and Over-The-Air or Over-The-Net updates for the software and firmware on the device. Similar to modern IT operations, these features provide better agility for the security staff to deal with vulnerabilities and security incidents, especially given scale of IoT.

Additionally, as depicted in the diagram, there are interdependencies among these areas.

Examples of interdependencies include:

- Through the process of risk assessment, sensitive assets may be given higher priority for protection through identity and access management (IAM) or monitoring services.
- When a monitoring tool alerts on a potential threat, IAM services may automatically be invoked to control access to affected assets, control connectivity to outside networks, etc.
- Sensitive or high-risk assets may require tighter maintenance inspection and update policies.

TAKING THE DIGITAL RISK APPROACH TO IoT

RSA is a market leader in the areas of risk, cybersecurity, identity and access management, and fraud detection at scale. Organizations around the globe rely on RSA products and services to address challenges in specific areas, but increasingly recognize that these solutions are broadly necessary to combat digital risks driven by digital transformation. At the highest level, the ability to coordinate and integrate high-quality technology is central to the ability to defend against new challenges.

At the highest level, the ability to coordinate and integrate high-quality technology is central to the ability to defend against new challenges.

Digital risks take many forms but there is a nucleus of challenges that encompass the great majority of scenarios that organizations face today. RSA research and customer interviews enabled the creation of eight critical risks—most of which are directly impacted by IoT. These are:

- **Manage third-party risk**—Adopt best practices for building a third-party governance program that helps your organization ensure ecosystem risks do not compromise business performance.
- **Manage distributed workforce risk**—Address the digital risk management challenges of a diverse, distributed, dynamic workforce, from privacy and compliance to authentication and access.
- **Mitigate cyber attack risk**—Prioritize threats to help coordinate an effective response to cyber attacks that helps minimize business impact.

- **Secure cloud transformation**—Gain visibility into cloud-based security risks, provide secure access to cloud applications and include cloud providers in third-party governance.
- **Evolve data governance and privacy**—Establish a data governance and privacy program that keeps pace with the complex regulatory landscape.
- **Build business resiliency**—Design resiliency into day-to-day business operations as organizations grow increasingly digital.
- **Manage process automation risk**—Manage digital risk when IoT, OT and other digital transformation technologies extend into manual business operations.
- **Modernize compliance programs**—Transform a spreadsheet-driven, check-the-box approach to compliance into a modern, integrated and agile function.

Specific to IoT, RSA is addressing new risks in ways that help organizations act strategically. These include:

- **RSA Archer® Suite**—The leading platform for Integrated Risk Management (IRM), with modules capable of identifying and managing the risks of IoT technology. The new **RSA Archer IoT App-Pack** is a customized tool for managing IoT risk, throughout the unique IoT lifecycle. These processes can be integrated with other IT security efforts such as cybersecurity and threat detection and response.
- **RSA IoT Security Monitor**—An "edge-to-core-to-cloud" IoT security monitoring solution, **RSA IoT Security Monitor** leverages open solutions for IoT edge management. Installed on IoT edge gateways and servers, it monitors any IoT deployment, no matter how diverse.
- **RSA SecurID® Suite** is a leading platform for Identity and Access Management (IAM) and Governance & Lifecycle (G&L). As IoT devices increasingly access people and systems, and especially data, **RSA SecurID Suite** delivers important capabilities that support diverse identities including IoT devices and systems, and maintaining rich access controls to ensure that devices do only what they are supposed to.
- **RSA NetWitness® Platform**—This leading Threat Detection & Response (TD&R) solution for IT systems features capabilities to ingest IoT data from many partners, including integration with RSA IoT Security Monitor. The convergence of IT and IoT presents an opportunity to leverage existing SOCs to protect against threats to IoT.
- **RSA Fraud & Risk Intelligence (FRI)** helps banks and merchants recognize and stop fraud while providing a seamless experience for customers. While these are generally human-driven interactions, RSA FRI omnichannel risk intelligence is exploring and anticipating ways in which fraud actors will try to exploit IoT to defeat fraud protection systems, and is integrating IoT risk factors into its analytic engine.

SUMMARY

As digital transformation drives fundamental changes in the ways that businesses operate—in areas as diverse as cloud, mobile, social, outsourcing, cyber risk, privacy, resiliency and automation—IoT is a thread that weaves through all of it. RSA understands these critical risks from a holistic perspective, and helps organizations implement programs that help across the spectrum. The world is changing quickly and everyone is required to adapt. Successful organizations understand that only a strategic digital risk approach will enable the full benefits of the next generation of digital technology.

For more information please visit **rsa.com/en-us/discover/internet-of-things**.

ABOUT RSA

RSA offers business-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 business 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**.