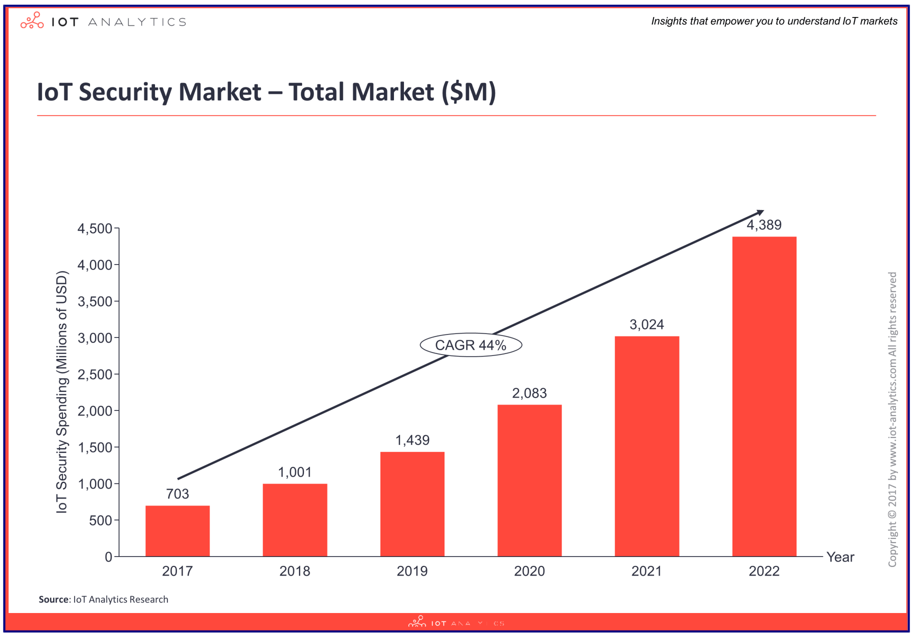
5 Things to Know About IoT Security

Insights From Ongoing Research on IoT Security

IoT Security is key for the secure development and secure operation of scalable IoT applications and services that connect the real and virtual worlds between objects, systems, and people. However, as our recent 3-part introductory series on Understanding IoT Security shows, IoT security is complex and the market landscape is largely fragmented with a host of vendors competing to address the opportunity.

In this article, we turn our focus to expand on 5 IoT Security insights gathered from our ongoing market research:

1. IoT Security Spending Is Rapidly Increasing



Global spending for end-users of 3rd party security solutions is currently estimated at $703M for 2017 and is forecast to grow at a CAGR of 44% to become a $4.4B market by 2022, driven by new regulation and increasing IoT adoption.

In addition to the security tools provided by IoT platforms (which is not part of this figure) the IoT security market is an aggregation of innovative startups and established firms such as global chip manufacturers, infrastructure providers, as well as cloud and enterprise software companies. There are at least 150 independent IoT security vendors addressing the challenges across all industries – of which Industrial/Manufacturing is the biggest segment for IoT security.

Example: A large auto OEM we talked to recently performed an assessment of factory vulnerabilities and concluded that there were significant gaps in today’s infrastructure. They expect to increase related spending significantly.

2. IoT Introduces an Increased Number of Security Threats

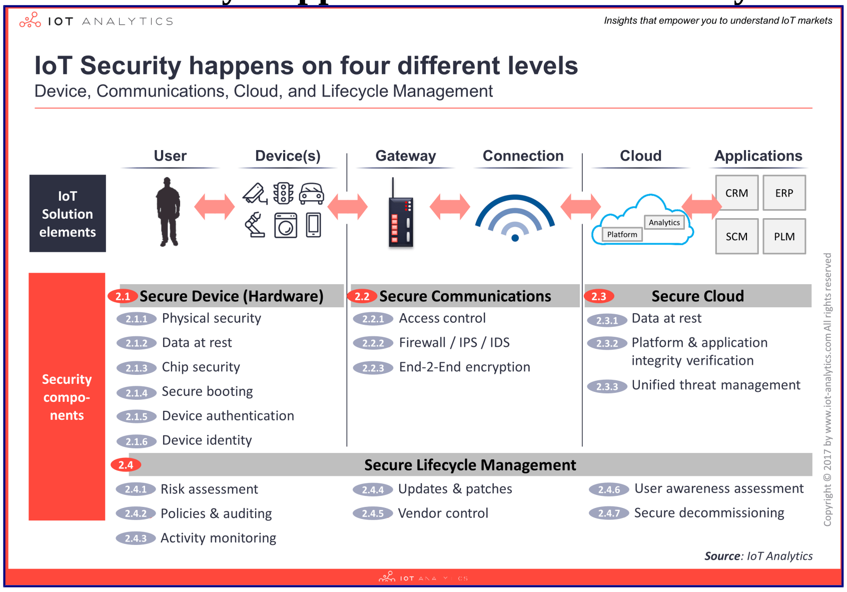
$$\text{Cybersecurity Risk} = \frac{\text{Threat Level} \times \text{Probability of Attack} \times \text{Points of Exposure}}{\text{Cybersecurity Measures Implemented}}$$

One of the big differences between the Internet of Things and previous internet technology is that the number of possible threats is much larger, due to the following (based on the above equation for the level of cybersecurity risk from Bosch):

- **More points of exposure**: The growing number of connected devices, applications, systems and end users mean more points of exposure.
- **IoT devices themselves become new attack vectors:** Every compromised device becomes a new possible attack point, which by definition means a higher probability of attacks.
- **Increased impact of attacks:** With more connected devices in many applications (i.e., hundreds of different use cases which all build on different standards, interact with different systems and have different goals – for example, see the Enterprise IoT Project List for 640+ different use cases), especially critical infrastructure applications where there is an increased impact of attacks (i.e., damage to the physical world and possible loss-of-life), the stakes are much higher for hackers which increases the threat level.
- **New threats from across the stack**: In addition, a more complex technology stack means new threats are possible from across the stack (i.e., from the different hardware, communication, and software elements – see Insight 2) which must be counteracted by the implemented cybersecurity measures and by experienced security professionals.

Example: A large industrial components manufacturer we recently talked to is now connecting legacy equipment on the shop floor to the internet to enable condition monitoring and predictive maintenance solutions. They concluded that by connecting the operational technology (OT) system and the information technology (IT) system – which were previously operating on two separate Wi-Fi networks within the same building – it creates new points of exposure that can be attacked. In particular, they noted that compromised 3rd party applications (i.e., from maintenance/service providers) could act as an entry point to the network and be taken advantage of to access other connected systems and bring production to a standstill.

3. IoT Security Happens on Four Different Layers


IOT ANALYTICS

Insights that empower you to understand IoT markets

IoT Security happens on four different levels

Device, Communications, Cloud, and Lifecycle Management

2.1 Secure Device (Hardware)
- 2.1.1 Physical security
- 2.1.2 Data at rest
- 2.1.3 Chip security
- 2.1.4 Secure booting
- 2.1.5 Device authentication
- 2.1.6 Device identity

2.2 Secure Communications
- 2.2.1 Access control
- 2.2.2 Firewall / IPS / IDS
- 2.2.3 End-2-End encryption

2.3 Secure Cloud
- 2.3.1 Data at rest
- 2.3.2 Platform & application integrity verification
- 2.3.3 Unified threat management

2.4 Secure Lifecycle Management
- 2.4.1 Risk assessment
- 2.4.2 Policies & auditing
- 2.4.3 Activity monitoring
- 2.4.4 Updates & patches
- 2.4.5 Vendor control
- 2.4.6 User awareness assessment
- 2.4.7 Secure decommissioning

Source: IoT Analytics

IoT solution architectures require multi-layered security approaches that seamlessly work together to provide complete end-to-end security from device to cloud and everything in between throughout the lifecycle of the solution. The 4 layers consist of:

- **Device:** The device layer refers to the hardware level of the IoT solution i.e., the physical "thing" or product. ODMs and OEMs (who design and produce devices) are increasingly integrating more security features in both their hardware and software (that is running on the device) to enhance the level of security on the device layer. *Security components include: physical security, data at rest, chip security, secure boot, device authentication and device identity.*
- **Communication**: The communication layer refers to the connectivity networks of the IoT solution i.e., mediums over which the data is securely transmitted/received. Whether sensitive data is in transit over the physical layer (e.g., WiFi, 802.15.4 or Ethernet), networking layer (e.g, IPv6, Modbus or OPC-UA), or application layer (e.g., MQTT, CoAP or web-sockets) unsecured communication channels can be susceptible to intrusions such as man-in-the-middle attacks. *Security components include: access control, firewall, IPS, IDS, and end-to-end encryption.*
- **Cloud**: The cloud layer refers to the software backend of the IoT solution i.e., where data from devices is ingested, analyzed and interpreted at scale to generate insights and perform actions. IoT cloud providers are expected to deliver secure and efficient cloud services by default to protect from major data breaches or solution downtime issues. *Security components include: data at rest, platform and application integrity verification.*
- **Lifecycle management**: Secure Lifecycle Management refers to an overarching layer with continuous processes required to keep the security of an IoT solution up-to-date i.e., ensuring sufficient security levels are in place from device manufacture, initial installation to the disposal of things. *Security components include: risk assessment, policies & auditing, activity monitoring, updates and patches, vendor control, user awareness assessment, and secure decommissioning.*

One should also note, at this point (Q4/2017) there is no single IoT security vendor that can provide the complete end-to-end out-of-the-box security solution. However, some companies offer more than others and together with their partner ecosystem some can provide a complete end-to-end IoT security solution.

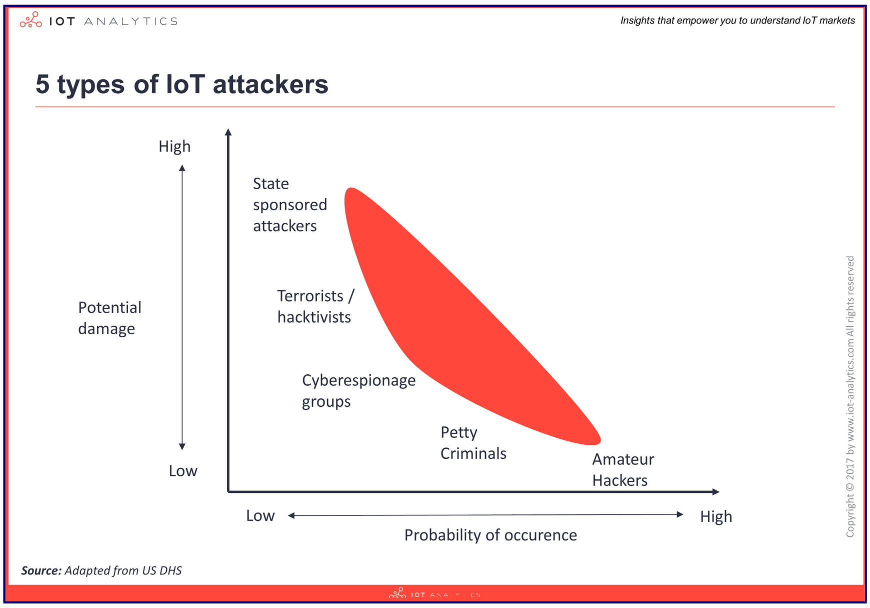
4. Increasing Automation of IoT Security Tasks

With forecasted growth to billions of IoT devices, manually handling security tasks (e.g., revoking certificates, isolating compromised devices), as is still the case in many solutions today, will not be feasible. Security automation techniques that merge security solutions and artificial intelligence are becoming more and more prevalent.

For example, next-generation activity monitoring enables advanced anomaly detection, building on sophisticated machine learning algorithms. One case includes objectively classifying ‘good’ files from ‘bad’ files based on mathematical risk factors, which means it becomes possible to teach a machine to make the appropriate decisions on these files in real time. This method drives autonomous decision making and changes the way an IoT device understands, categorizes, and controls the execution of every file.

Example: Their approach begins with the collection of a massive amount of data, from which they identify a broad possible set of attributes for a file. Converting these attributes to numerical values means they can be used in mathematical models. Vectorization and machine learning are applied to these models to eliminate the human impurities and speed up analytical processing. Mathematicians then develop statistical models that accurately predict whether a file is valid or malicious enabling them to discover and quarantine threats at the endpoint.

5. Cyberespionage Groups and Petty Criminals Are the Most Common IoT Attackers



The five main types of IoT attackers today are:

1. **Amateur hackers:**e.g., script kiddies, hobbyists.
2. **Petty criminals:** e.g., low-level cyber criminals.

3. **Cyberespionage groups:** e.g., organized syndicates or crime groups such as Armada Collective, Black Vine, GreenBug.
4. **Terrorists / hacktivists:** e.g., professional, non-state actors such as Oxblood Ruffin or political hacktivists.
5. **State sponsored attackers:** e.g., foreign espionage via state-sponsored sabotage and traditional adversarial nation-states e.g., Russia, China.

Each class of attacker may have different abilities, capabilities, and goals – whether on an individual or group basis (i.e., aggregating resources to work together). Given the same tool different classes of attackers may achieve different outcomes e.g., experienced cyber criminals can evade deep packet inspection tools or IDS signature detection tools whereas new hobbyists may not.

However, cyberespionage groups with vast resources and highly skilled petty criminals are the most common type of IoT attacker. In many cases, they have developed advanced malware with the ability to mutate and evade detection for longer on IoT networks or they leverage DDoS attacks as a means for blackmail.

Example: Armada Collective is an example of a traditional cyberespionage group that has recently demanded that businesses pay thousands of dollars (predominantly in Bitcoins or via PayPal) or run the risk of having their services brought down by crippling cyber-attacks. Although the actual members of the original Armada Collective appear to be locked up in a European jail, some enterprising individuals that are financially motivated are continuing to use the group’s name for extortion.