Internet of Things has arrived

For many internal auditors the Internet of Things (IoT) may not yet be a central area of focus of their work, but there's a good chance that the IoT is already present in their personal lives. Wearables such as the Apple Watch or smart speakers like Amazon Echo, devices or “things” that are connected to the internet, are prime examples of how quickly IoT connectivity has become a feature of modern life.

There are an estimated 23 billion connected devices in the world, or three for every person on the planet, according to Statista, and this is forecast to rise to more than 75 billion by 2025. That is a relatively conservative estimate. Intel has said it expects there to be as many as 200 billion connected devices by as early as 2020.

IoT may seem like a new and overwhelming concept, but the internet itself is a global network of connected computers, or things, that has been in operation since the early '90s. IoT expands this network to a greater number of devices.

Much of the boom in the IoT will be in personal products, but there is vast scope for industrial and commercial applications, many of which already exist. These applications will help to increase efficiencies, reduce costs, improve revenues and reduce operational risks. Of course, they will also dramatically change organisations' risk profiles.

As with the adoption of any technology, organisations must understand how they can exploit IoT to their advantage, either by being an innovator or early adopter in their sector, or by rapidly assimilating advances made by other organisations.

Intel estimates that by 2025, the total global worth of IoT technology could be as much as $6.2trn; two industries anticipated to feel the greatest impact are healthcare and manufacturing, which could account for as much as three-quarters of that value.

In healthcare, some of the most immediate applications are in patient monitoring, such as home-based tele-health IoT devices that can remotely monitor patients' heart rates and other metrics, alleviating pressure on emergency support services. Adding sensors to medicines and delivery mechanisms, including minute ingestible sensors, allows doctors to keep accurate track of whether patients are sticking to their treatment plans.

In manufacturing, companies are increasingly interested in the use of low-cost sensors for the preventative maintenance of machines, while in the oil and gas sector these networked devices can determine in real-time the pressure of oil wells, removing the need for engineers to conduct periodical manual checks.

Cyber versus physical

New IoT applications are being developed all of the time and the opportunities these represent cannot be ignored. As organisations increasingly harness such networks and in new ways, they and their internal audit

functions must understand the associated risks.

To illustrate the risks presented by IoT in a commercial context, consider first the smart home. All manner of appliances, including radiators, ovens and kettles, may be wirelessly connected to a network. The inhabitant may remotely command the heating to warm the home before they return. As convenient and potentially energy-saving as this may be, if someone were to hack a smart home they could control the heating or anything else that is connected to the network. In 2017 ethical security researchers SureCloud did exactly this, hacking a CloudPet, a “smart toy” that enables family and friends to send messages to a child, and ordering cat food via a nearby Amazon Echo.

Other than the risk of failing to exploit the IoT, which applies to all disruptive technologies, at a basic level the security risk is an extension of cyber security. However, while the aim may be to steal or hold sensitive data to ransom, as is the case with many traditional cyber-attacks, IoT opens up the potential to hijack and manipulate the physical environment using the organisation's IT network as an entry point.

For instance, the Stuxnet worm that was discovered in Iranian nuclear facilities in 2010 not only gave attackers (alleged to be a collaborative effort between the US and Israeli governments) access to industrial data, they were able to physically operate machinery at a number of sites, destroying 984 uranium-enriching centrifuges.

In essence, IoT risk is a convergence of traditional IT risks related to the security of the organisation's computer network and risks related to operating technology – that is, task-specific physical systems. In many cases, these physical systems are infiltrated via the organisation's enterprise IT system (e.g. Stuxnet is believed to have been deployed with a phishing email) and so strong cybersecurity protocols will help to significantly mitigate IoT risk, although the potential security weaknesses of hardware and associated firmware should not be underestimated.

Given the speed at which the IoT is being adopted for industrial/commercial purposes, one of the most fundamental steps for internal audit in understanding how IoT risk is being managed is having a clear view of how such technologies are being deployed in the organisation today, and how they are likely to be used in the coming years.

The following considerations for internal audit have been grouped under five broad themes.

Opportunity and strategy

1. Given the potential for the IoT to reduce costs and increase revenues and efficiencies, is the business putting such technologies in place?
2. Does the organisation understand the ways in which IoT can be harnessed to its advantage?
3. Has a cost-benefit analysis been conducted and are there plans to act on its findings?
4. What is the IoT strategy?

What and how?

1. If IoT is already in place, what does it look like and how is it being deployed?
2. Has an IoT inventory been taken so that relevant stakeholders understand exactly where in the organisation it features and what it's being used for?
3. Is this inventory periodically updated?

Risks and response

1. Has a risk assessment been conducted to determine how these technologies could be attacked and subverted?
2. Does this take into consideration the outcome of such attacks, e.g. data loss, mission-critical processes going offline, or workers and the public being put at physical risk?
3. Are continuity and response plans in place in the event of such an attack occurring?

Security protocols

1. What is the maturity of the organisation's cybersecurity governance and controls?
2. Are measures in place to prevent and detect internal and external attacks to the IT network, e.g.

    a) correct firewall configuration,

    b) patch management and software updates,

    c) access rights management,

    d) penetration testing,

    e) network scanning and breach detection, staff training and awareness?

3. To what extent are these likely to be effective in preventing IoT networks from being compromised and identifying when they have already been compromised?

4. Have security considerations that are specific to the IoT hardware (and firmware/software) been accounted for, as distinct from the IT network?

5. If so, are these being appropriately managed?

Interoperability and expandability

In many cases IoT technologies will be retrofitted to existing operating technologies, such as sensors and networks fitted to factory machines. Also, an IoT system will likely be part of a much larger network within the organisation and this interoperability, or lack thereof, is seen as one of the most significant hindrances to IoT.

1. Internal audit should therefore be thinking about the extent to which this is being accounted for.
2. Are sub-networks (including devices manufactured by different companies and using different operating systems) able to communicate with each other?
3. Can the data being collected through IoT networks be exploited as part of any broader big data strategy in the organisation?
4. Is the scalability and interoperability of IoT being designed into systems?
5. Are weaknesses at the intersection between different IoT and adjacent non-IoT IT systems being considered?

The IoT will develop rapidly over the next decade and organisations will have to act quickly in order to make effective use of such networks to gain a competitive advantage. We recommend, therefore, that internal audit takes a broad view of cybersecurity as it continues to encompass a larger pool of devices and “things” that were previously offline.

Further reading

For a more in-depth look at IoT-specific security protocols and risks take a look at the below:

Industrial Internet Consortium's security framework

Open Web Application Security Project's IoT security guidance