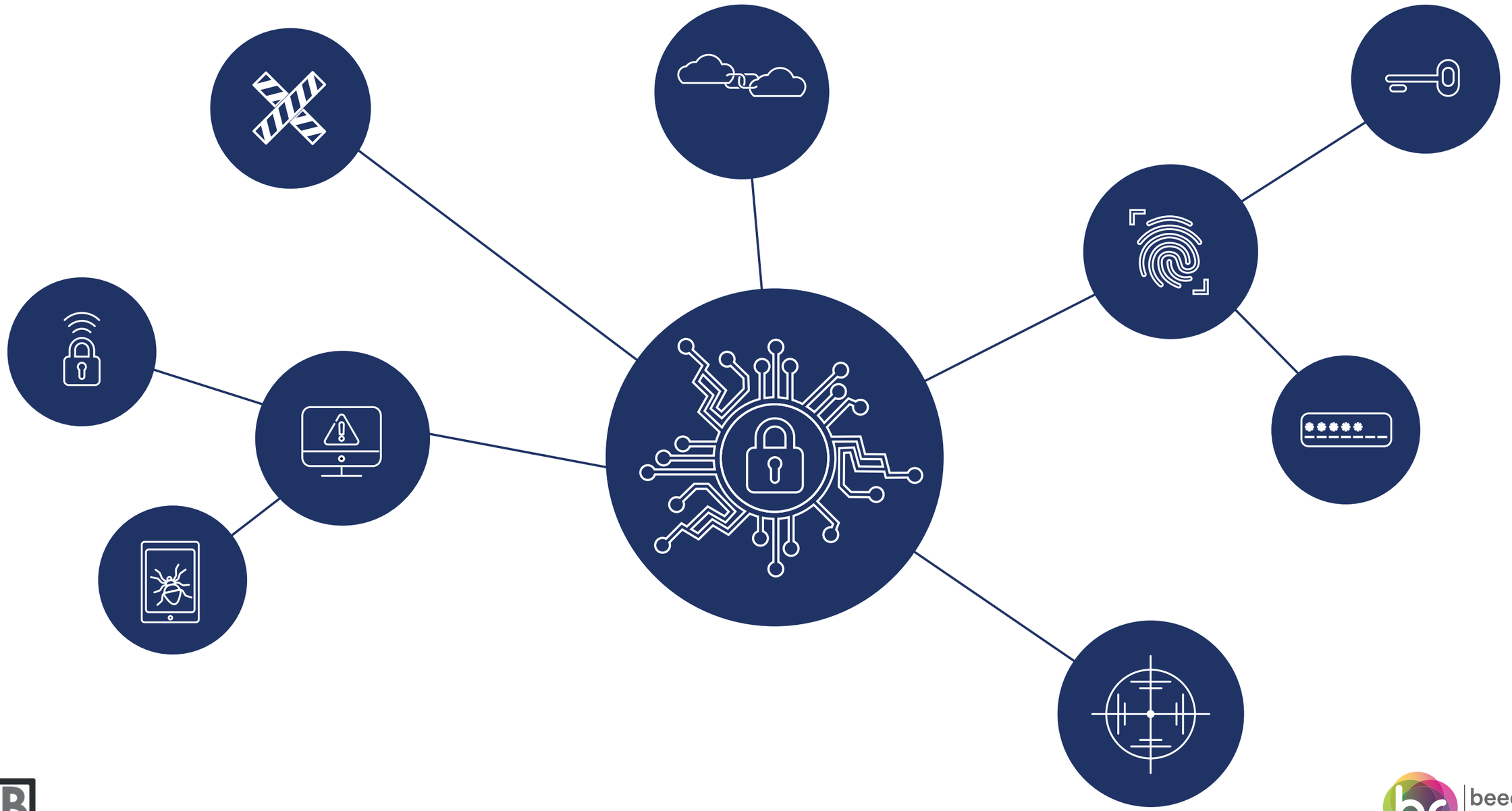
iot&devicesecurity



internetofbusiness
Demystifying IoT and explaining the connected world

beecham research
Shaping the IoT future

Introduction »

» The distributed denial of service (DDoS) attack on Dyn, a Domain Name System (DNS) service provider, in October 2016 was a milestone security attack of the year. The reason for this prominence is 3-fold. First, the DDoS attack reached a new record volume exceeding 1Tbps. The previous record was between 620-655 Gbps from the DDoS attack on Krebs Security, a popular and widely respected security blog. Secondly, the source of vulnerability was consumer-facing Internet of Things (IoT) devices such as baby monitors, printers and IP surveillance cameras. These devices, infected with Mirai, transformed into botnets that launched the DDoS attack. Thirdly, the DDoS attack on Dyn took down its customers including the cloud infrastructure leader, Amazon Web Services, among other cloud based solutions and e-commerce companies.

It is a logical expectation that IoT devices, legacy or new, add another level of complexity to enterprises' security posture. Already, enterprises face a shifting landscape of external and internal security risks and have a finite budget to build their arsenal of tools and skills to mitigate the risks as best as they can. With IoT deployments, many enterprises have started experiments without involving security professionals to provide the necessary framework to ensure deployments are also secure. With the upcoming General Data Protection Regulation (GDPR), there is an opportunity to use this imminent compliance issue to direct the starting conversation about IoT deployment to include data privacy and privacy. We recommend that the IoT community also brings to the table, IoT technology capabilities, industry knowledge, enterprise digital transformation perspective, and security strategies.

In an ideal not too distant world, we recommend that enterprises think about securing the IoT as good practice not only from protective instincts about data security and privacy. Instilling a security by design to IoT deployment lays the foundation for businesses to begin to quantify trust so that customers have a metric to measure and benchmark digital enterprises. It leads to enterprises being able to monetise this trusted reputation as a business in a digital future of connected, artificial intelligence-enhanced, and self-organising societal systems.

This paper is organised in 5 sections

1. Securing the IoT
2. Enterprises' overall security objectives and challenges
3. GDPR is another set of acronyms for the IoT community
4. A new metric is essential to measure 'trust' in IoT
5. Key questions you should ask the IoT community

This brief builds to 3 main messages for the IoT community

1. Evangelise security into an enterprise's overall IT business objective.
2. Provide directed GDPR implications for IoT deployments.
3. Facilitate the technology solution to build the new trust metric «

Challenges in securing the internet of things

» Defining security is an ambitious task. The concept of security encompasses nine key elements as shown in Figure 1 (overleaf).

In the evolving IoT markets, security is not just referred to security of information, but it expands into all the complexity of the IoT vision. Before discussing more in detail the challenges in the IoT security, it is also important to highlight that security issues in the IoT strongly relate to privacy and trust issues. Having said that, it is important to stress that installing security capabilities does not necessarily implies right to privacy and trust relationships. Privacy and trust go beyond the technological domain into ethics and legislation. Therefore, an IoT security strategy should take into consideration multidisciplinary aspects to be effective.

But, concentrating the effort of this section on the technological aspects of security in the IoT, it is important to de-construct an IoT solution in its components to see the need of security. Figure 2 (overleaf) shows the hierarchical level of an IoT solution.

All levels of an IoT solution need to be suitably secured. But, it is also important to assess the value for the different layers to ensure that costs and benefits are well understood.

More complexity is introduced in the moment in which we see the Internet of Things vision as the enabler of interconnected smart contexts – spaces -. The solution does not engage with business problem only, using one type of device, one type of connectivity, one protocol and one set of data. There are then several different devices, using different protocols, using different types of connectivity, using different sources of data. The points of attacks are then multiplied as showed in the Beecham Research Threat Map in Figure 3 (overleaf).

The enormous challenge of the IoT strategy and solution designer is using the Threat Map to identify the right approach to protect the smart context in which he or she operates. This means that the security priorities differ according to industries, or for this purpose of paper, according to the type of stakeholder needs:

- Consumer-facing applications such as those in smart homes.
- Industrial applications such as those in manufacturing, or those in critical infrastructure such as electricity grids, telecommunication networks or even transport infrastructure.
- City-wide applications and services such as those within smart cities domains.

Even from these 3 types of stakeholders, the traditional enterprise security framework certainly does not fit into the considerations that each IoT system requires. We recommend that securing the internet of things needs to be a fit-for-purpose strategy not only from technology and applications perspectives but also from an enterprise's business objectives angle. «

Fig.1 Essential Pillars in Security

Authentication

Authentication is the act of confirming the truth of an attribute of an entity or a single piece of data. In contrast with identification, authentication is the process of actually confirming the identity or confirming that data arriving or leaving is genuine.

Authorisation

Authorisation is the function of specifying access rights to resources and ensuring that any requests for data or control of a system is managed within these policies. During operation, the system should use the access policies to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected), and what actions should then be taken on any disapproved access, for example logging failed requests to enable analysis of where failed events originated.

Availability

Availability has two definitions within the IoT and M2M domain. Firstly as with mainstream information assurance, the system must ensure that data and resources are available in a timely manner for a set percentage of the time (eg. 99.99% uptime availability). Secondly in the IoT it is critical that many devices are available, or retain their critical functionality, even if the system has undergone an attack. For example a home heating system must retain core functionality even if the device's communications have been compromised.

Confidentiality

Confidentiality is a set functionality that limits access or places restictions on certain types of information with the goal of preventing unauthorised access.

Identification

Identification is defined as ensuring a device or service can be specifically and uniquely identified without ambiguity. This may take the form of an IP address, global unique identifier, functional or capability identifiers, or data source identifiers.

Integrity

Integrity ia a critical measure in information assurance and is defined as ensuring consistency or lack of corruption within an electronic system. In this context it is required that data cannot be modified without detection.

Non-repudiation

Non-repudation isz an aspect of authentication that enables systems to have a high level of mathematical confidence that data, including identifiers, are genuine. This ensures that either a transmitting or receiving party cannot later deny the request occurred (cannot later 'repudiate') and ensures data integrity can flow around the system. In most IoT/M2M systems a data hash algorithm, such as SHA2, is seen as sufficient today although this is likely to be insufficient in the future.

Root of trust/ Chain of trust

A root of trust ia an immutable process within a system on unique identifiers, cryptographic keys and on-chip memory, to ensure the device cannot be compromised at the most fundamental level. The chain of trust extends the root of trust into subsequent applications and use cases.

Secure update

Updates, by their nature are significant security threats and ensuring only correctly signed firmware updates can be applied is critical for long life-cycle devices.

Fig.2 Levels of Hierarchy in an IoT Solution

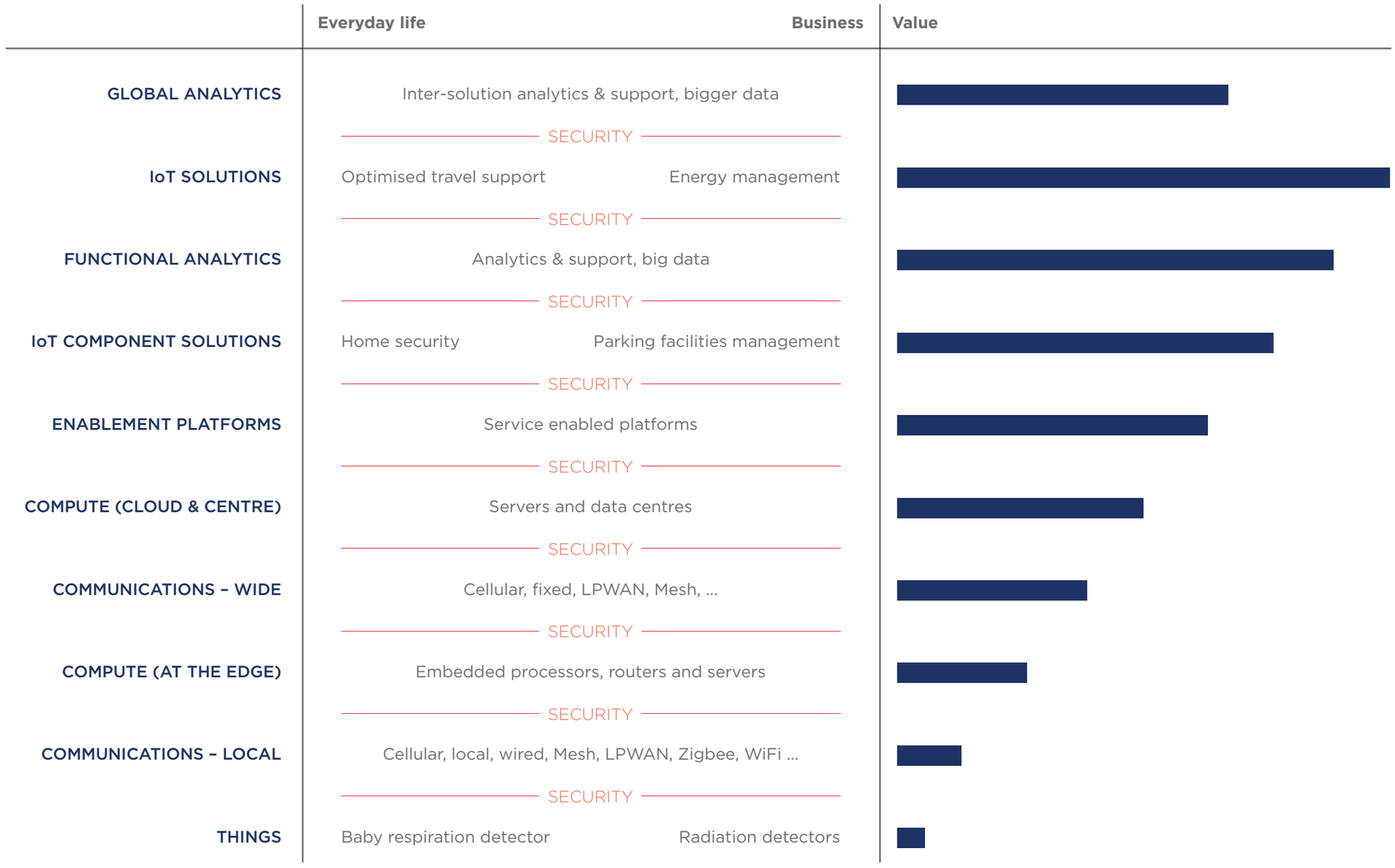
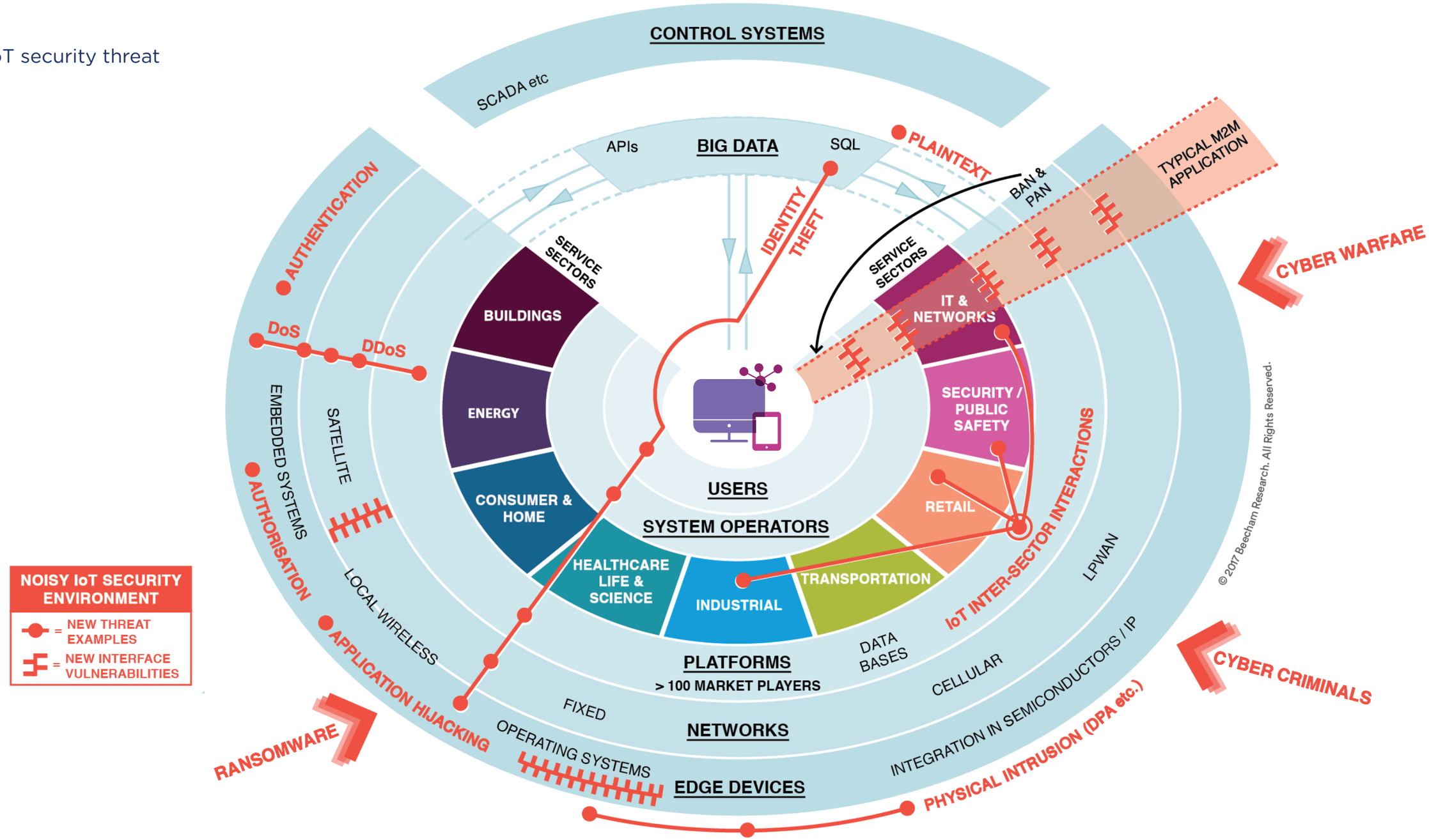


Fig.3 IoT security threat



A 'fit for purpose' security paradigm for IoT must align with an enterprise's aspirations

» A fit for purpose security strategy for IoT reflects an enterprise's digital aspirations with its internal obstacles. A typical enterprise faces 3 key operational challenges in security operations, even without the additional complexity of securing the IoT. Adding in IoT specific risk challenges, the traditional enterprise security framework becomes insufficient. For example, traditional security technologies often only take care of networks, endpoints and increasingly users. However, it is often difficult to account for both human and machine behaviours. We recommend that enterprises must incorporate security risks in IoT into their overall security strategy, aligned with their digital aspirations. Along with aspirations, a security strategy must adapt to each stage of their digitalisation.

There are 3 common operational challenges facing the security teams. The most prohibitive factor for 'more' security is that security investment, as part of an overall IT budget, is finite. The share of information security to total IT spending varies between 10-15% and may increase temporarily but rarely enjoy a sustained hike in the proportion. A finite budget implies a stringent cost-benefit analysis for each security issue before an investment allocation will be made. From a security perspective, allocation of budget is often tied up with other IT transformation initiatives such as those about cloud migration, e- and mobile- commerce strategies, customer experience improvement, and including IoT projects. Without a Chief Information Security Officer (CISO) who sets a security strategy for its organisation and ideally who also directs security conversations at the board level, security and privacy are often left as an afterthought, resulting in enterprises using imperfect products to incorporate protection into their IT infrastructure. The recent example of even the most well-prepared company such as Maersk was still hit by the Petya ransom-ware. Despite setting out its digital strategy with the recruitment of both a Chief Digital Officer and a CISO as Maersk embarked on using IoT technologies, it still suffered a disruption to their operations. The saying 'it is not if but when' about being part of a cybersecurity attack is not a niche. The challenge is implementing this as part of an overall business strategy.

A second internal operational challenge within the security teams is that in-house cybersecurity skills and experience will always lag significantly behind the technological might and commitment zeal of threat actors and other security risk factors. According to the 8th Global Information Security Workforce Study conducted by ISC2 in 2017, the projected shortfall for cybersecurity professionals continued to widen to 1.8million by 2022.

The commitment of threat actors, whether they are nation or non-nation states, is usually more persistent and with more resources of funds, technology and time, than your typical enterprise security teams. Against these committed and well-funded threat attackers, a typical enterprise' approach towards cybersecurity risks is about risk management. The challenge for security teams is to do more with less; which in turn requires security capabilities to simplify, automate and even democratise security operations. Adding in the complexity of security issues in IoT, the traditional perimeter based enterprise approach becomes a sub-optimal approach. The current mindset of security team's return on investment remains within the boundaries of traditional enterprise framework, protecting the perimeter of networks, end-points and users. With IoT adoption, the equation for security investments must expand to include the very real reputational costs and possible liabilities.

A 'fit for purpose' security paradigm for IoT must align with an enterprise's aspirations (cont.)

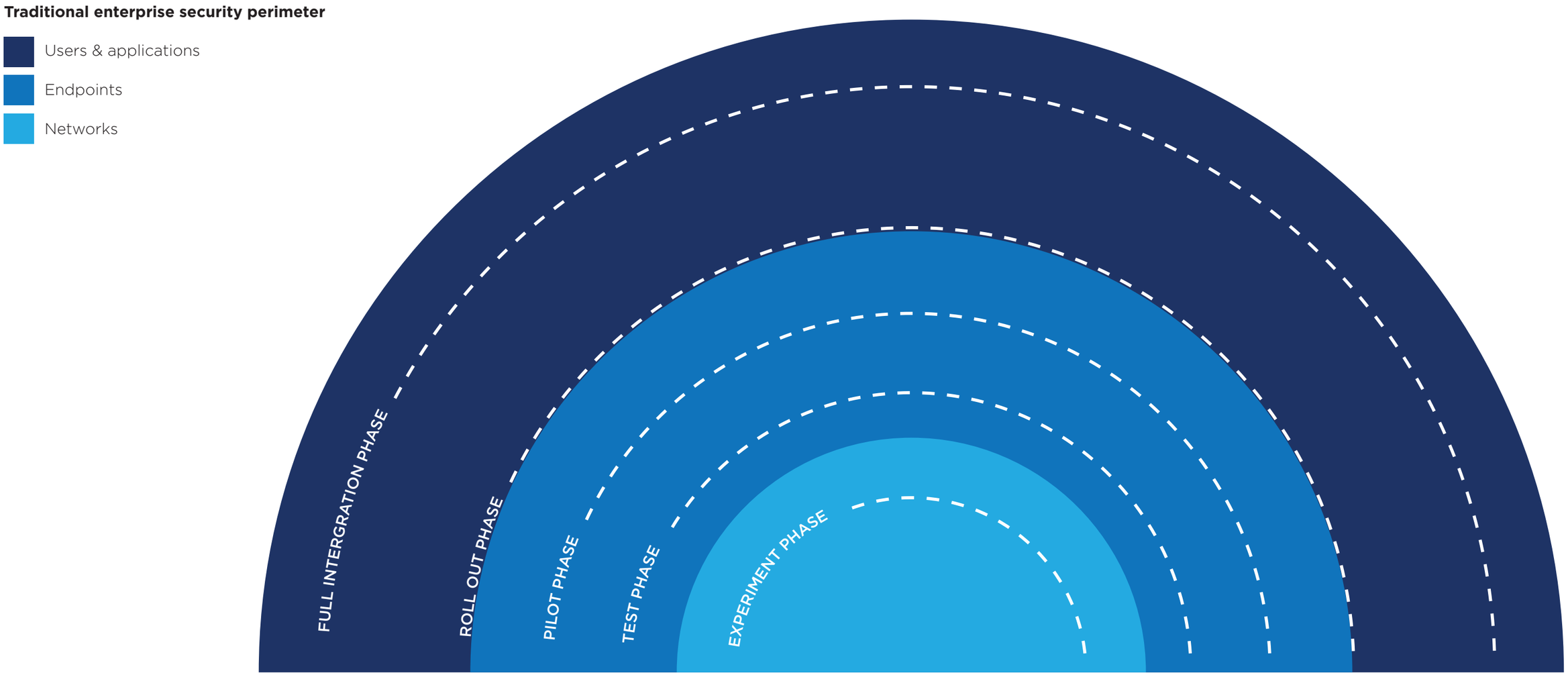
A third operational challenge facing security teams is the lack of success in arguing for security investments to protect IoT projects and to communicate this within IT teams, business units and the board. When security concerns are embedded right from the start of IoT project investigations or deployment can widen the scope of benefits in security team's cost benefit analysis. More importantly, the IoT community could do well to articulate not just the security concerns but the associated cost related to a breach at every stage of a technology deployment phase. Figure 4 (overleaf) updates the threat map with the deployment phases, adding the phases of an IoT deployment project to security team's list of priorities at the Experiment, Test, Pilot, Roll-out and Full Integration phases.

At each stage of an IoT deployment project, the security priorities differ according to the scale and desired outcomes. For example, the desired outcome for an enterprise starting to use IoT technologies at the experiment stage is to ensure the built IoT system works. The security priority at this stage is about the IoT device. The security issues may be related to software (protecting against malicious code from being loaded to the device) or device authentication (identity management, credentials protections), or simply ruggedized devices against physical tampering.

As the IoT project moves beyond the experiment stage to test and pilot, roll-out and full integration, the number of touchpoints increase substantially. For example, even at the stage of testing that includes a handful of users and applications, the network, end points and users within a traditional enterprise security scope become those touchpoints that need to ensure protection. At roll-out or full implementation, the IoT project will touch other IT initiatives such as cloud transformation or customer experience transformation. Security priorities thus focus on data protection and privacy, raising the importance of data encryption, at rest and in transit.

One of the key learning points from an IoT development cycle is that the trade-off between performance, cost and protection changes over the project phase. A crucial operational challenge in operationalising security processes in enterprises deploying new technologies including IoT is how to embed security mind-set from the beginning. We recommend enterprises align their security strategy with its digital aspirations because the risk management equation can include an additional potential revenue component. The upcoming GDPR in 2018 is an important behaviour modifier. «

Fig.4 Aligning security strategy with IoT deployment phases



GDPR influences businesses to embed data protection by design

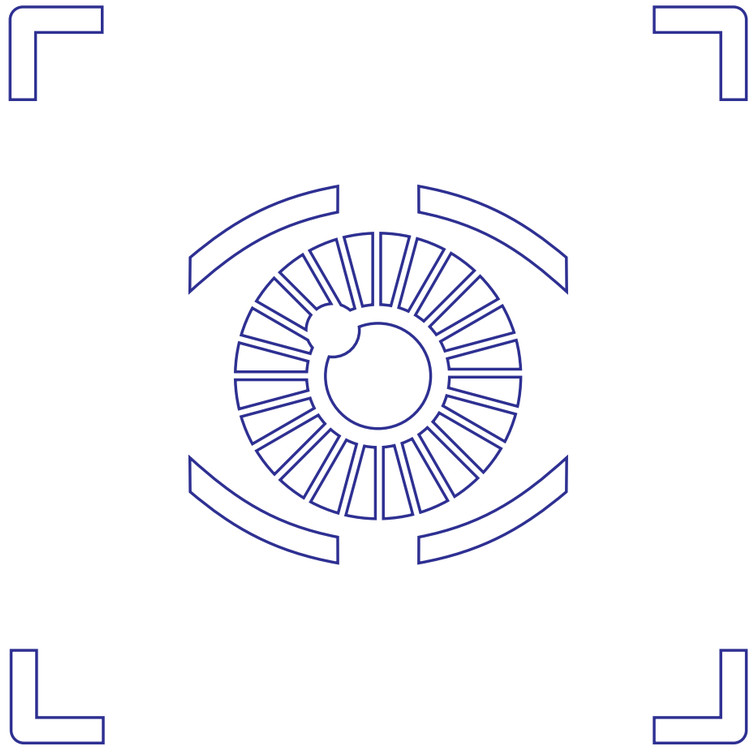
» GDPR has been adopted by the European Union in April 2016 to better protect EU citizens' personal data privacy. It will replace the current and more narrowly applied Data Protection Directive (95/46/EC) with a single regulatory framework applicable to all EU and non-EU businesses that process personal data of EU citizens. The aim is to encourage businesses to entrench data protection by design practices and to demonstrate in auditable steps that ensure EU citizens' right to data protection and privacy. In the event of a breach, businesses have 72hours to report the breach to supervisory authorities and affected individuals. This means that businesses must have the technical and organisation structure to detect report and investigate the breach. Penalties for non-compliance are much higher under GDPR than in the current directive; up to €20m or 4% of global annual revenue.

The UK government reaffirmed its commitment to implement GDPR in a report published in December 2016, following the EU referendum outcome of the UK leaving the union. As such, UK businesses must also prepare to be GDPR compliant come 25th May 2018. According to the advice from UK's Data Protection Authority, Information Commissioner's Office (ICO), GDPR requires UK businesses to demonstrate how they have complied with the principle of 'accountability' to protect individual's data privacy.

What this means for securing the IoT is that for every IoT device that is put into the system, the enterprise must be able to prove that it has done so with data protection and privacy in mind. This so-called 'security-by-design' requires a complete change from bolting security on after an application or code been developed. It requires, for example, building an IoT app that is secure, high performing, and can scale. GDPR is so often the hot topic in the infosecurity sector but its relevance to IoT deployment is less articulated by both security and IoT communities.

Complying with GDPR also has another practical implication for IoT deployments. The financial penalties are decided based on security processes. This means that the enterprise must demonstrate that it has taken the optimal steps to ensure the flow of information and data within the IoT systems are data security and privacy protected. GDPR's more stringent regular and the higher financial penalty suggest that requires enterprises first to be aware of what IoT devices are out there, to be able to authenticate communication handshakes, to detect a breach, to respond and mitigate the breach. The IoT community must articulate the security processes that occur within IoT systems to help enterprises navigate the compliance of GDPR come 25th May 2018.

We recommend that enterprises embrace the compliance of GDPR as the external factor to trigger an organisation-wide soul searching exercise. Become a trusted digital enterprise relevant in a fully automated, artificially intelligence enhanced future. In such a scenario, trust becomes another vital metric that digital enterprises will have to report as part of their overall corporate strategy. The IoT community has the knowledge and responsibility to lead the market by helping to define this and to educate enterprises on the safe and secure way to adopt IoT technologies. «

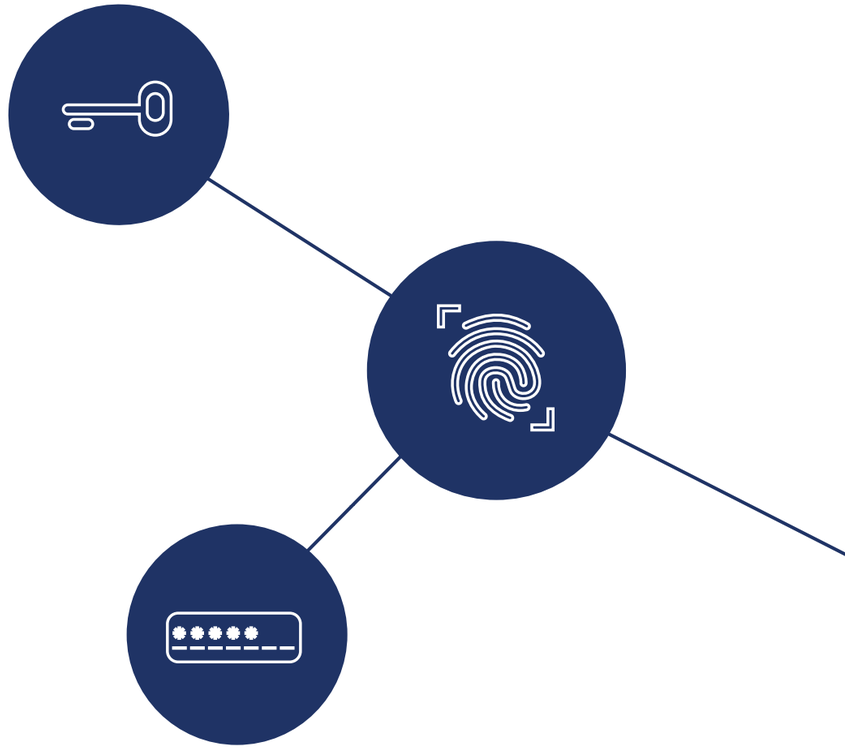


New metric to measure 'Trust' in a digital society

» As mentioned earlier, security issues in the IoT strongly relate to privacy and trust issues. For example, in the case of industrial IoT, trustworthiness of data is key. Without sufficient security, there can be no trust. In September 2016, the Industrial Internet Consortium (IIC) published a report detailing a security framework for IIoT. It defines clearly that safety, reliability; resilience, security and privacy define the trustworthiness in IIoT systems.
In another example, IoT devices rely on a trustable base of hardware like to chip to establish their system's root of trust, a set of unconditionally trusted functions, to execute a simple instruction of a secure boot. The application of blockchain technology within IoT systems reflects the desire to, for example, establish IoT identities, as a way to support the creation of trust.

However, the measurement of whether an enterprise has done what it promised it would do remains a vague fledgling idea. Just as net promoter score (NPS) measures customer satisfaction, we recommend this metric to be based around customer experience. This customer experience is tied to how an IoT solution has supported enterprises' efforts to provide data security and privacy assurances. For example, a wearables manufacturer is transparent in the way the device has been manufactured, its app and data storage are secure, and privacy notices comply with GDPR requirements.

The IoT community would benefit from incorporate privacy technology within their portfolio. Current opt-in/out method of receiving consumer consent is not sustainable in a digital lifestyle universe where services cross over various domains. Backlash from consumers can occur easily, for example, from ad-blocking. Inaccurate customer segmentation as a result of broad aggregations and limited signals suggest a market gap for a more accurate reflection of consent. More importantly, settlement mechanism needs to be developed via insurance companies and other stakeholders for clearing individual's data sharing thresholds with perceived privacy. The IoT community, in leading these conversations, is in the position to further develop this new trust metric, for what it means for an enterprise to be 'trusted' or be 'privacy-centric'. «



Enterprises' questions for the IoT community

Following the many IoT security frameworks released in 2016, we recommend that enterprises demand that their IoT partners also address the security questions that support their efforts to improve their overall security posture including supporting IoT deployments, to accelerate compliance of GDPR, and eventually to monetise security investment in a digitalised era. Beyond questions about the functionalities of IoT solutions, we recommend enterprises to also ask these practical security questions:

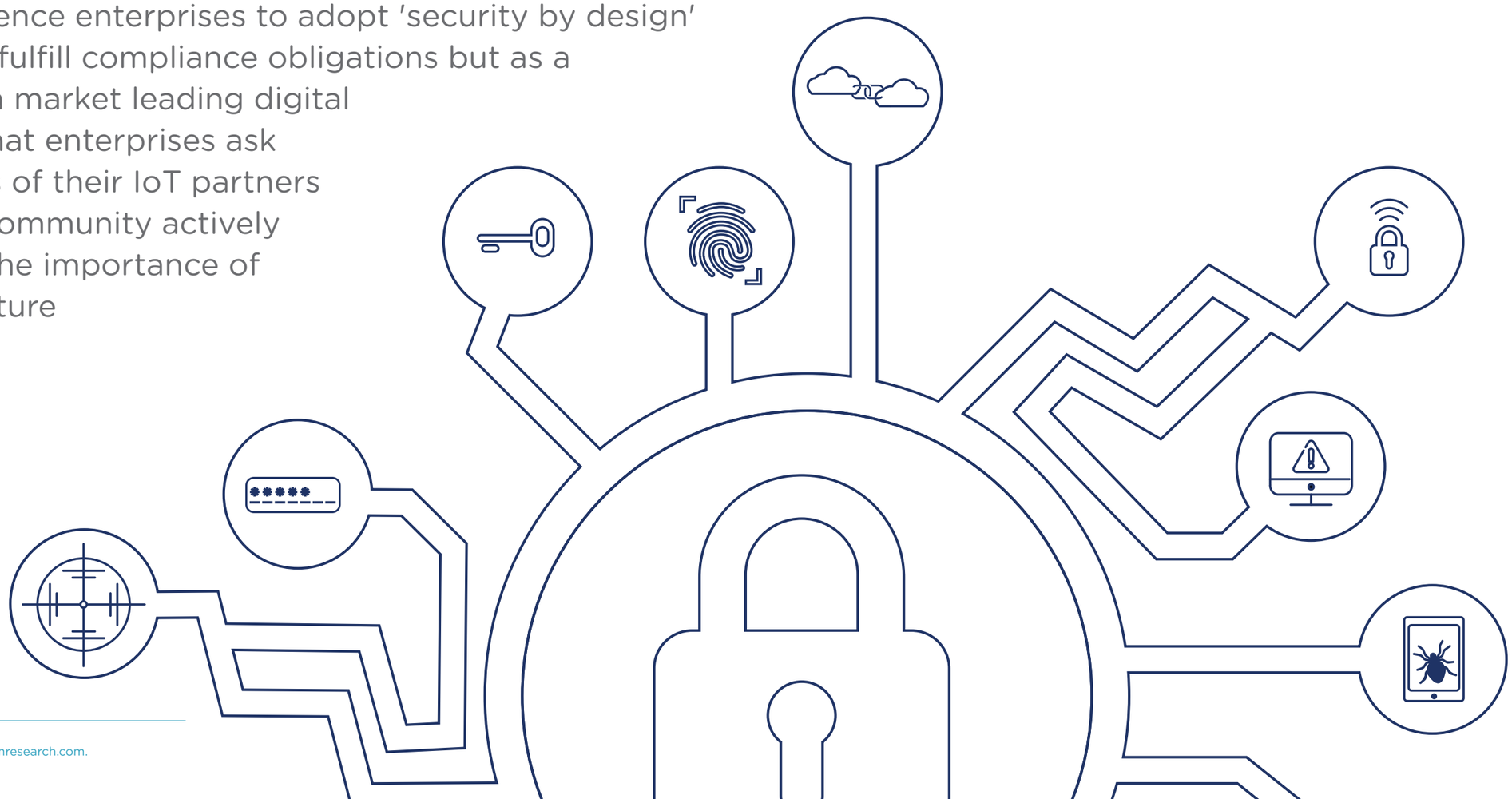
1. How will you support my on-going security processes already in place, accounting for my existing security infrastructure and limited human resource constraints?
2. How will your solution help me discover where my data is, how to protect it, and how to ensure privacy in real time throughout the IoT system?
3. How will my IoT project be integrated with my existing IT initiatives specifically in cloud adoption?
4. How many security professionals exist in your organisation and how are their inputs reflected in your IoT solutions? Do you also practice 'security by design'?
5. Which IoT security guideline(s) do you follow?

The IoT community on the other hand, must be prepared to address the following 3 key conversation topics with their customers on operationalising security within IoT deployments. These are the 3 key conversation topics to be had; all of which require a separate brief:

1. Reducing the security challenges facing enterprises today.
2. GDPR's implications on IoT trials and deployments.
3. The opportunity in the convergence of privacy technologies and IoT systems.

Conclusion »

» Security issues in IoT systems add to enterprises' security burden. With more devices expected to be connected to the internet, enterprises will continue to struggle to improve and optimise their security posture. As enterprises seek to optimise their security investment by doing more with less, for example, their return on investment calculation should include an element of security investment monetisation. We expect the IoT community to contribute to the creation of such a 'trust' metric that measures and tracks enterprises' trustworthiness in a digital world. We expect GDPR to be the change agent to influence enterprises to adopt 'security by design' best practices to not just fulfill compliance obligations but as a differentiating factor for a market leading digital enterprise. We demand that enterprises ask security related questions of their IoT partners and in turn, that the IoT community actively educates enterprises on the importance of emphasising security posture in all IoT solutions. «



iot&devicesecurity

5th-6th December 2017
Munich, Germany

Ensuring high end-to-end security processes when building IoT

The only forum to discuss the end-to-end security process, from Network to Device, and help you define the features and products you need for your use case. A series of Keynotes and interactive sessions will be complemented by technical sessions, workshops, demos, training that showcase exactly how to secure IoT.

Join a vendor-neutral platform to exchange best practice on creating agile, resilient and vigilant security apparatus with CTOs, CIOs, CISOs and Heads/Directors of Security, Cybersecurity, Networks, Architecture, Compliance, Information Security and more.

To register visit:
W internetofbusiness.com/events/iot-device-security

internetofbusiness
Demystifying IoT and explaining the connected world

Internet of Business is an international media organisation expert in the fast growing Internet of Things (IoT) sector. We provide platforms for thought leadership, high-level engagement, analysis and brand visibility through market specific events, insightful content and industry news.

IoB's digital publication features News, Insights and Analysis on the business and technology opportunities around the Internet of Things and the connected world and is relevant to both end user and vendor communities.

We offer rich, informed content and insights from leading IoT luminaries, thought leaders and industry experts across a mix of industry verticals including retail, manufacturing, health, transportation, insurance and energy.

W internetofbusiness.com
E info@iob-media.com
@InternetofBiz
linkedin.com/groups/6700306/profile.

beecham research

All research and data has been undertaken by **Beecham Research** for and on behalf of Internet of Business.

Beecham Research is a leading market research, analysis and consulting firm, specialising in the worldwide M2M / Internet of Things market. We are internationally recognised as thought leaders in this area, where we have deep knowledge of the market dynamics at every level in the value chain.

We are experts in M2M/IoT services and platforms, and also in IoT solution security, where we have extensive technical knowledge. We explore the impact of the Internet of Things in various sectors and are also the leading analysts in satellite M2M.

Our clients include component and hardware vendors, major network/connectivity suppliers (cellular, fixed, satellite, short/long range), system integrators, application developers, distributors and enterprise adopters in both B2B and B2C markets.

If you would like to discuss your M2M/IoT needs with us please feel free to contact us at:

T 020 7749 1944
W beechamresearch.com
E info@beechamresearch.com
@beechamresearch
linkedin.com/company/beecham-research.

Yiru Zhong is principal analyst at Beecham Research where her twin focuses in IoT are in cybersecurity and privacy issues in IoT applications, and in smart energy. Her research experience started in the telecommunications market pre-iphone era, before extending to the M2M sector in 2009. Previously, she was senior industry analyst at Frost & Sullivan, covering IoT and security topics.
In her previous role, she had also guided digital transformation initiatives in such industries such as smart energy, connected cars and transportation sectors.
She is currently studying for a CompTIA security+ certification.

E yzhong@beechamresearch.com