The IoT Industry Action Plan to Reduce the Cost of Security

How Prevention Over Cure and a Culture of Collaborating on Best Practice Can Shift the Economics of IoT

psacertified™

Munich RE

Department for Digital, Culture, Media & Sport

UCL

FORESCOUT

January 2022

Table of Contents

Introduction

We live in an age of convergence and digital transformation. New tech is coming together with new expertise, to create new opportunities.

This era of digital transformation has largely been made possible by the Internet of Things. Long heralded as the next step in our journey towards a connected reality, the Internet of Things, or IoT, is already reshaping our lives.

A connected world is undoubtedly an exciting one in which to live, but it will only fulfil its potential if security is optimised, and there are several factors currently making the cost of security a concern for the silicon vendors, software providers and device manufacturers that are so vital to its success.

To address the most pressing challenges, a collective industry effort is needed. We are only as strong as our biggest risk area, and as cyber risk grows, no one party can be held responsible for delivering a more secure IoT. Instead collaborating and agreeing on common concepts is what will enable the ecosystem to align on how to fix the security holes that exist across the supply chain. Only through collective best practice will IoT accelerate digital transformation.

It is with this in mind that this report shares insight, knowledge and collective best practice from some of the leading minds working across the IoT ecosystem - from government to cyber insurance firms to academia.

Here we present an action plan for reducing the cost of security and forging a more powerful connected future.

“A secure IoT is only possible if consistent frameworks, testing and best practices are made accessible to all that need them, without the associated costs becoming a barrier to entry.”

— David Maidment, Senior Director, Secure Device Ecosystem, Arm (PSA Certified co-founder)

Contributors:

Tim Davy

Cyber Security Specialist, MunichRe

Munich RE

Veena Dholiwar

Cyber Security Expert, Department for Culture, Media & Sport

Department for Digital, Culture, Media & Sport

Madeline Carr

Professor of Global Politics and Cybersecurity at UCL

UCL

David Maidment

Senior Director, Secure Device Ecosystem, Arm (PSA Certified co-founder)

psacertified™

Elisa Costante

VP of Research, Forescout Technologies

FORESCOUT

Sally Eaves

Global Foundation for Cyber Studies and Research

How and Why Security is Becoming More Crucial

As industries, businesses and economies become increasingly reliant on the connected economy, its potential as the bedrock of digital transformation continues to accelerate. Yet with great opportunity also comes great risk. And as IoT adoption grows, so does the cyber risk from bad actors wanting to exploit it.

On average there are 5,200 attacks per month on IoT devices, with 7 million data records compromised daily[1]. The average cost of a successful IoT device attack is more than $330,000[2] and it's estimated that by 2025 cybercrime damages will total over $10 trillion[3].

The impact of a cyber breach on the bottom line is well documented; yet the true cost of insecurity spans far beyond the cost of the attack itself. There's a raft of associated elements to consider - trust, reputation, consumer churn - and we need to look at embedding the value of security correctly in order to address these different cost issues.

So beyond the bottom line, what are the other risks a cyber breach can cause?

The Convergence of Digital and Physical

IoT introduces the capacity for the digital world to affect the physical world in an unprecedented way. Critical infrastructure is reliant on it, and many of our medical systems, smart cities and connected homes are powered by it. It poses a potential threat to physical safety and even life in ways we've not experienced before, heightening the risk and liability for organizations, governments, individuals and ecosystems to mitigate.

"The IoT begins to blend worlds of security and safety in ways we haven't seen before. It also brings additional risks to both of those factors. One of those new risks is the capacity of threats to impact the real world - to change something in the physical world. With that, we introduce a new load of liability that we haven't considered within the context of cybersecurity - physical damage or in the worst case, loss of life."

— Madeline Carr, UCL

UCL

"IoT are the controllers that are used for managing the distribution of oil or energy; our critical infrastructure relies on IoT and OT devices. Cars are becoming computers with wheels. So, when we speak about risk coming into an organization now we have a much wider perimeter that we need to look at."

— Elisa Costante, Forescout

FORESCOUT

IoT Security is Now an Issue of Business Resilience and Continuity, Not just Technology

Adding to the convergence of real-world and digital risk is the prevalence of IoT across sectors and territories. It's not just large enterprises that are affected by cybersecurity; small and mid-sized enterprises (SMEs) across all industries and verticals are challenged with a growing cyber threat, and the world is still learning to navigate it.

"The mass gathering of data and the aggregation of that data can change its value and purpose. These are very significant concerns for organizations that collect any type of data. And ultimately these are the issues in the context of the IoT that we need to have in the forefront of our thinking about business resilience and continuity."

— Madeline Carr, UCL

UCL

"We have digital assets now but also expanded supply chain challenges from a risk perspective. Where does liability start and stop? Starting at the core, we talk about Security By Design a lot and having trusted components within an organization or system allows us to compartmentalize where we'd see that risk."

— Tim Davy, Munich Re

Munich RE

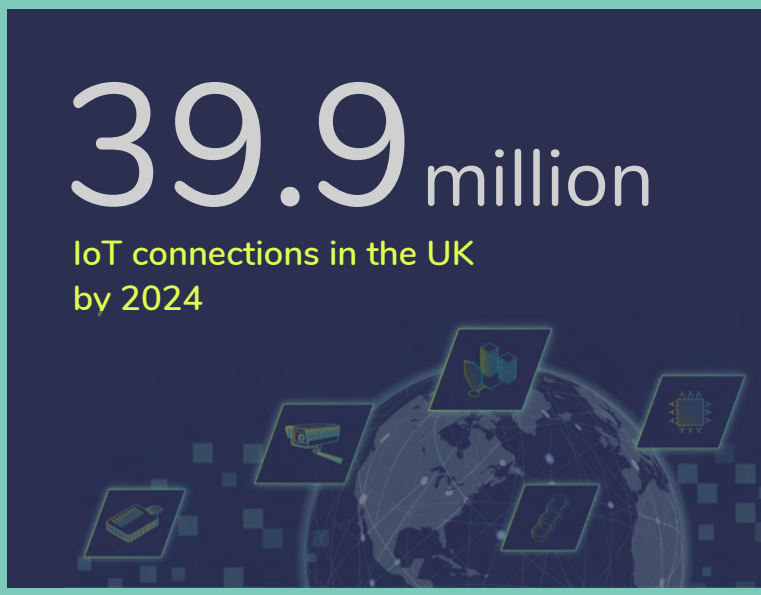
The Anatomy of Devices is Increasingly Complex

The threat profile of an interconnected device is both significant and nuanced, which adds to the complexity of securing the IoT. A recent Forescout Technologies study into IT stacks (the basic technical level for making devices communicate) shines a light on the scale of the problem. They found around 100 different vulnerabilities in any stack. That's 14 pieces of code used by 400 different vendors in 100 different products which results in billions of devices being impacted by one disruption. Tracking where the risk is coming from across the supply chain and identifying how to tackle it becomes ever more difficult.

Homes are Becoming Extended Parts of Our Enterprises

There is an impressive readiness for and adoption of IoT, accelerated by the pandemic. By 2024, it is estimated that the number of IoT connections in the UK will increase to 39.9 million[4].

COVID-19 has increased our reliance on technology, increased the number of connected devices people are using and so increased the associated attack surface. It has also accelerated the digitization of offices and industries as new measures are put in place to monitor and manage distributed workplaces. This in turn is diversifying the risks consumers face and the threat vector for the IoT - a vector that will continue to grow as advancements in technology such as 5G improve user experience and encourage further adoption.



The Cost of Security Investment vs The Cost of Insecurity

Addressing the cost of security investment versus the cost of insecurity is a hugely complex problem that cannot be solved by one party. It is an ecosystem challenge: a challenge with high stakes.

The cost of cyber-attacks and cyber risks are well documented. The effect on the bottom line is clear. Fines, lost data and customer trust all add to the bill – a bill that, as previously mentioned, will propel the cost of cybercrime to $10.5 trillion by 2025.

IoT Security Economics

The economics of IoT security as it stands, i.e., an industry that's predicated on cost-per-unit and time to market, means there's an ongoing battle between cost of security implementation and cost of inaction/insecurity. For OEMs to implement the requisite security techniques and solutions there's an added cost to bear, especially when parties are starting from scratch and not from a common foundation. Keeping the Bill of Materials (BOM) low to ensure a strong profit margin has long been the defacto priority, which conflicts with the capital investment required to build in security.

Not only can return on investment (ROI) be difficult to quantify, but there's not always an obvious market incentive for investing - at least continuously - in security. As The PSA Certified 2021 Security Report highlighted, the need for upfront capital presents a clear barrier. Over half (52%) of decision makers consider the additional cost of security to be a top barrier to implementation and a similar number (54%) cited 'uncertain ROI' and a 'lack of buy-in' as a blocker to ongoing security investment.

52% consider the additional cost of security to be a top barrier to implementation

54% cited 'uncertain ROI' and a 'lack of buy-in' as a blocker to ongoing security investment

**PSA Certified 2021 Security Report*

With over 1,000 different laws globally there's also an additional complexity challenge to navigate. But new enforceable standards and baseline requirements, whilst complex and often fragmented, are helping to create new frameworks for a more secure IoT. Vendors need to understand worldwide law, not just local legal requirements in order to ensure compliance and optimise security - all of which can have an impact on time to market, and in turn ROI.

"Return on investment can be really difficult, as it can be hard to quantify but also there isn't a clear market incentive for investing further in security in all sectors. The sectors where there is, will be the ones to drive the take up of security and amortize the cost."

— Madeline Carr, UCL

But the true cost of insecurity transcends far beyond the bottom line and financial metrics. The reputational risk a data breach poses, along with the indelible threat to customer confidence and trust that comes with it can quickly translate into a loss of customers, revenue and investment. Over half (58%) of those surveyed in the 2021 PSA Security Report expected their reputation to be damaged by a cyber attack. Add to that the cost of restoration and investigations, coupled with the huge strain on resources required to repair from a cyber incident, and the case for shifting IoT security from a hygiene factor to a headline feature has never been stronger.

Over

58%

expected their reputation to be damaged by a cyber attack

So How Can We Reframe the Narrative around Security, Cost and ROI?

Four industry imperatives:

1. Move Away from Security as a Software Problem: Security in Device Components

A fundamental aspect to IoT security is the components with which IoT devices are built. Security is dependent on hardware protection in the silicon chip at the heart of the device, and if we skip this vital step, we expose both users and manufacturers to vulnerabilities. This problem is largely overcome by careful chip design, to which there are two costs associated. One is the cost of designing it which requires divisions of security experts architecting best practice and is often prohibitively expensive. The second, of course, is building and deploying the security into the products in question.

> **"A lot of the innovation in cybersecurity in the past has focused on software. It's that chip architecture and chip design that's fundamental in making a step change in IoT security."**
>
> — Madeline Carr, UCL

Having a clear vision of what we can do to reduce the security risk and how to develop that within the industry is mission critical to helping shift the economics around IoT security. Talking not just to the manufacturers but also others in the supply chain about ensuring security for the consumer is crucial.

2. Adjust the Economics around Cost of Security

Consumers, businesses and governments now mandate more robust device-level security. Increasingly consumers expect security to be part of the device they buy and not a premium they should have to pay for: **"1 in 5 consumers already check security; however, we found that a high number of consumers expected that a high level of security was already built into a device."** — Veena Dholiwar, Department for Culture, Media & Sport.

When combining an increasingly complex cyber risk landscape with growing consumer expectation, the economics of security must move away from cost-per-unit and towards having a security baseline to protect against the most common hacks.

How can this be achieved?

• Building on Trusted Components and Embracing Easy-To-Use Frameworks, Evaluations and Certifications.

Combined with increased threat modelling, these ingredients are crucial to untapping IoT's potential. OEMs can reuse certificates to save money and resources, and expertise can be shared across the value chain. Similarly, an industry-led set of guidelines or frameworks can help to fast track best practice.

"Having trusted components within an organization or system helps insurers to compartmentalize risk and reduce the cost of inaction. With more trusted components, comes greater business resiliency and more understanding of supply chains that keeps the cost of failure to a minimum."

— Tim Davy, Munich Re

Munich RE

"In the UK, we started working with industry to understand what the current security practices were and what was deemed to be common good practice. This led to the publication of an agreed Code of Practice for Consumer IoT Security that led to the development of ETSI standards on consumer IoT security (EN 303 645). That set consistency and a baseline, enabling industry to be aware of their security expectations, and create a level playing field."

— Veena Dholiwar, Department for Culture, Media & Sport

Department for Digital, Culture, Media & Sport

• Legislation, Standards and Regulations

Policy and legislation provides justification and incentive for businesses to mandate and implement higher levels of security, especially in sectors where there isn't a clear ROI. Creating best practices that map across territories in an ever-changing global supply chain will help to uplevel security and ultimately drive consistency across markets.

"Having standards and regulations in place in industries helps put the yard stick in the right place and sets the right direction." — Tim Davy, Munich Re

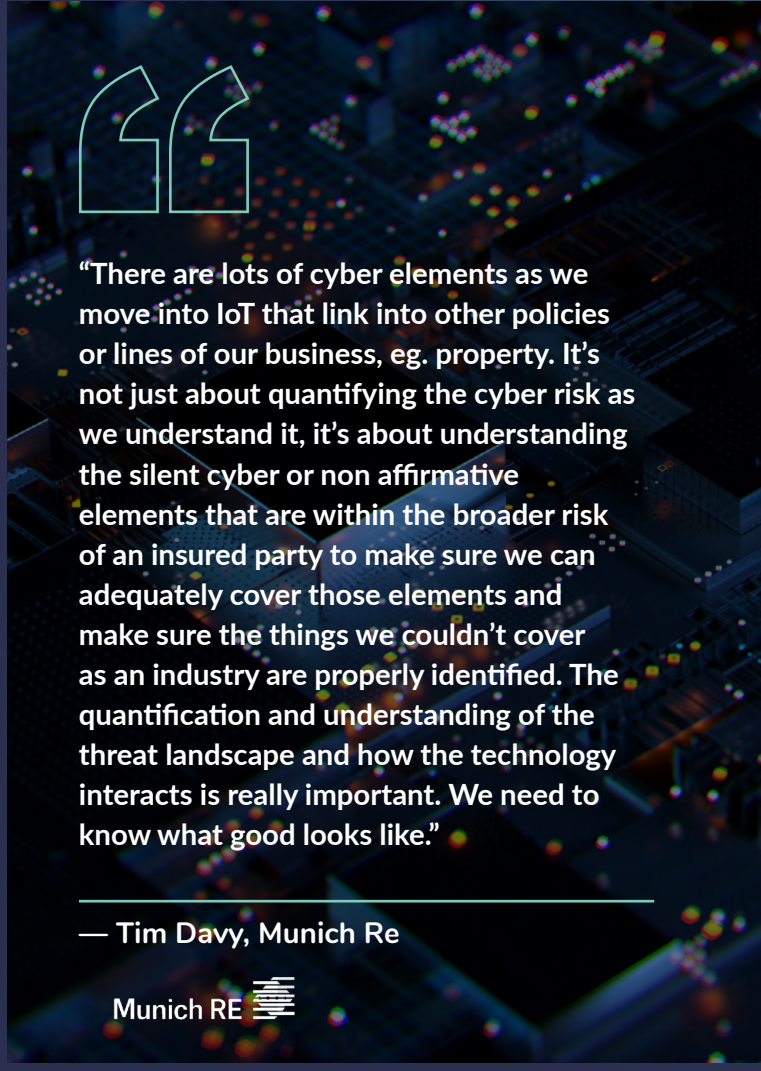
• Democratizing Skills and Enabling Scalability

By designing based on the Root of Trust, there's a democratization of security and skills. Companies can implement security best practice and differentiate around it, making it possible for all parties to benefit from built-in security goodness. This is what will ultimately help security to thrive on a very big market of people that want it and embrace it.

3. Modeling Known and Silent Risks in order to Mitigate Them

When it comes to identifying, modelling and establishing a quantifiable level of risk in IoT, the picture is extremely complex. Not only as a result of the sheer scale and complexity of the IoT and its supply chain, but because of how it dovetails almost every industry, sector and line of business.

Determining the quantification of risk for a single device is also more nuanced than simply the number of vulnerabilities. It's a question of how critical the devices are and how trusted the vendors are. All of these factors need to be considered when identifying, assessing and mitigating potential risks.



"There are lots of cyber elements as we move into IoT that link into other policies or lines of our business, eg. property. It's not just about quantifying the cyber risk as we understand it, it's about understanding the silent cyber or non affirmative elements that are within the broader risk of an insured party to make sure we can adequately cover those elements and make sure the things we couldn't cover as an industry are properly identified. The quantification and understanding of the threat landscape and how the technology interacts is really important. We need to know what good looks like."

— Tim Davy, Munich Re

Munich RE

"There's a misconception that risk is simply the number of vulnerabilities that I have on that device. Whilst there's of course a relationship between those things, they are not to the same factor. If I have a vulnerability, but I also have the right hardware mechanism implemented, then the risk factor is reduced. Without the right hardware security built in, the risk accelerates if a device is connected to the internet."

— Elisa Costante, Forescout

<) FORESCOUT

4. Uplevel and Translate Technical Literacy

Building certified equipment with trusted components is fundamental to negating the threats posed by bad actors, but how do the purchasers of equipment or the people who don't understand the detailed technical subtleties of this pick that up? How organizations and c suites uplevel that understanding and translate that goodness into trust and confidence is what will enable markets to scale. Education and awareness is already building beyond enterprise security - further facilitating and translating that technical literacy will play an important role in mitigating future risk.

"While more technical literacy is always helpful, board members need to move beyond being intimidated by technology and recognize that they already have the skills they need to evaluate and mitigate against business risk – which is how cyber risk should be understood in that context."
— Madeline Carr, UCL

Conclusion

The challenges ahead of us may be clear: from SMEs to large enterprise and the different convergences we're seeing in terms of technology coming together, rate of change and bad actor activity. But what can also be seen is the art of the possible made real by bringing together best practice in cutting-edge business, cutting-edge technology, education and research; different bodies bringing different dialogue and voices to the fore so that everyone can be heard, as well as the education around that.

The success and continued growth of the IoT is dependent on collaboration - a proactive, coherent and collective approach.

"Good collaboration expands beyond the electronics industry and beyond the boundaries of what we often think about. We have a global vision and we're finding a way for the world to collaborate on secure digital services. That's a huge opportunity across the board - from Government, industry best practice, enterprises, all the way through to consumers."

— David Maidment, PSA Certified

psacertified™

The world is ready for effective, far-reaching IoT security. Technical know-how and a reframed economic model around IoT must come together so that the overall cost of IoT security can be reduced. Reducing these costs will increase IoT security adoption across the board, helping to further mitigate risks, as will increased cyber insurance. Certification will also continue to play a key role. Ultimately, when these things converge and collaboration and trust are placed at the centre of any IoT security action plan, the IoT can be considered a secure environment for the world to thrive in.

One which can act as an agent of positive digital change.

One which will see the art of the possible made real by co-creation and collaboration; reducing threats by the convergence of the positive and not the negative.

Top Tips for Mitigating the Cost of Best Practice Security

#1

Make Trust the Foundation of a Secure IoT

Trust is the biggest currency of our time. And the future of both IoT security and digital transformation depends on it.

"One of the critical factors to the success of IoT will undoubtedly be consumer trust and confidence. People need to trust that their data is being handled in a responsible way. It's virtually impossible for an individual to know what happens to the data once it's connected and shared, and that's something that we need to address otherwise it will limit the positive impact of the IoT. The question of ensuring there's a level of accountability for data handling will be critical."
— Madeline Carr, UCL

"This is about deploying connected devices and digital services at scale. So building trust in devices, as well as in the data and the service they generate is essential for successful digital transformation. We can't think about the cost of an attack, but need to consider the hesitancy as well as the rate of adoption of security. Organizations and industries are going through the learning curve of understanding that you can create business cases around this and deploy with confidence. And in turn that will help to engender trust."

— David Maidment, PSA Certified

psacertified™

#2

Collaborate to Accumulate: Establishing a Baseline of Best Practice

In a sector as nuanced as IoT it helps to view the ecosystem as a village coming together over a common cause. In this case, the inhabitants coming together are the insurance pillar, technology pillar, governance pillar and legislation pillar. When these come together and the collaboration model extends beyond the electronics industry, a baseline for IoT security best practice can be established to catalyze digital deployment globally.

"There has been a lot of international collaboration. Cyber security doesn't stop at the border. Having that international influence is vital. Some of this took place through the development of ETSI, but other countries such as Australia and India have also published their own guidelines that align with ours, and Singapore has also launched a scheme which aligns with our approach."

— Veena Dholiwar, Department for Culture, Media & Sport

Department for Digital, Culture, Media & Sport

#3

Take an Assumed Breach Stance. We're only As Good As Our Biggest Threat Area

"When things do go wrong, it's important to always take an assumed breach stance. This means having the market capital and business capital in place to navigate a possible breach. It's not just large enterprises that are affected either. Add to that the expanded supply chain challenge from a risk perspective - where does the liability start and stop? The work of PSA Certified and other initiatives are helping to drive trust and that's a key pillar for insurance."

— Tim Davy, Munich Re

Munich RE

#4

Best Practice as a Minimum Requirement

"We're mandating requirements for a minimum level of cyber security for consumer connectable products, to give clarity to device manufacturers on good practice."

— Veena Dholiwar, Department for Culture, Media & Sport

Department for Digital, Culture, Media & Sport

#5

Seek External Validation: The Role of Certification

Establishing best practices that insurers, businesses and the broader ecosystem can rely upon is vital in the context of quantifying risk. Independent certification - through the chip, software and the device - provides an objective view of standardized security, validating that a deployment is based on secure components and devices.

"It's fundamental that security is built in a consistent way at the chip architecture level, so the supply chain can easily understand and measure levels of security. Having independent evaluation is also important. As an industry we can't mark our own homework, it needs to be reviewed by independent labs to show it conforms with particular norms and levels. Aligning to Government and regulation best practice is mission critical."

— David Maidment, PSA Certified

psacertified™

Turn These Actions Into Your Everyday Practice.

LEARN MORE ABOUT HOW THE PSA CERTIFIED ECOSYSTEM CAN HELP YOU

Thank you

References

1. Source: Semantec
2. Source: Irdeto Global Connected Industries Cybersecurity Survey
3. Source: Cybersecurity Venture
4. Source: Ofcom

psacertified™