The IoT Revolution:
Uncovering Opportunities, Challenges and the Scale of the Security Threat

Introduction

The Internet of Things (IoT) does not represent the future of enterprise IT. It's actually already here, transforming business processes, accelerating productivity and driving growth in industries as diverse as healthcare, retail and government. The industrial IoT (IIoT) offers arguably some of the greatest opportunities for innovation, redefining how organisations in industrial and manufacturing sectors operate by making them more efficient, cost effective and customer-centric.

Gartner claims there are over 8 billion connected "things" in use today, and the figure will top 20 billion by 2020, including over 7 billion specifically for business use.

Yet, as organisations embark on ambitious digital transformation projects to harness the power of IoT and IIoT, they also expose themselves to the risk of attack. Part of the challenge stems from the fact that much of the IIoT world is firmly rooted in operational technology (OT). OT teams very often do not consult security teams and are not primarily concerned with data availability, integrity or confidentiality. This can leave dangerous gaps in cybersecurity if IT-OT siloes are allowed to persist. If not managed properly, IoT projects can drive an explosion in unsecured endpoints – endpoints that could be used as a stepping stone into corporate networks en route to sensitive customer data and IP; hijacked to turn into botnets; or sabotaged to potentially put employees and customers in physical danger.

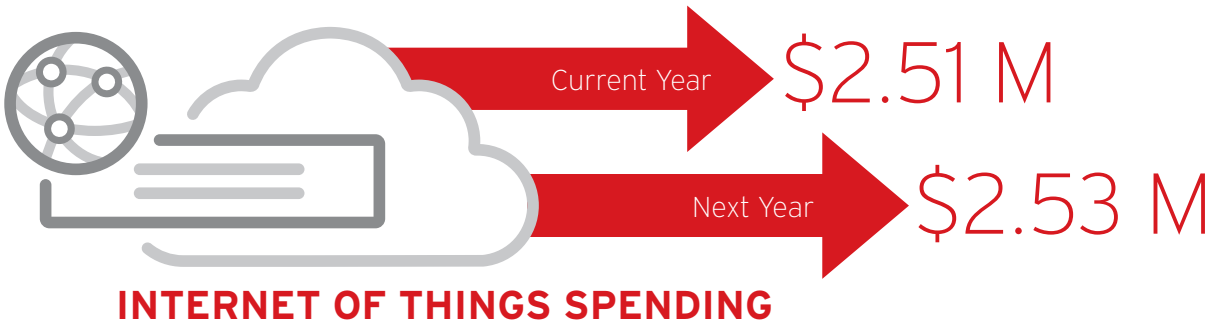
Trend Micro has followed this area closely for many years, producing pioneering research over recent months into the security challenges associated with emerging intelligent transport systems, industrial robots, and connected cars. But we wanted to pull back a little and find out more about the kinds of IoT projects being driven by global organisations, their key challenges and perceived threats, along with hard data outlining the frequency and type of attacks they've already experienced.

With this information, we can begin to understand where the key risks lie in IoT initiatives, what organisations should do better, and where security vendors need to step in to help mitigate those risks. European organisations in particular must now ensure they build security into every new IoT system, or risk the wrath of both GDPR and NIS Directive regulators.

Methodology

Trend Micro commissioned Vanson Bourne to interview 1,150 IT and security decision makers in the US, UK, France, Germany and Japan. Respondents hailed from organisations ranging from 500-999 employees to 5,000+ across 16 separate sectors. Roles ranged from CISO/CSO and IT security manager to CIO, IT manager, Chief Risk Officer (CRO), CTO, and Data Protection Officer (DPO).

The IoT landscape

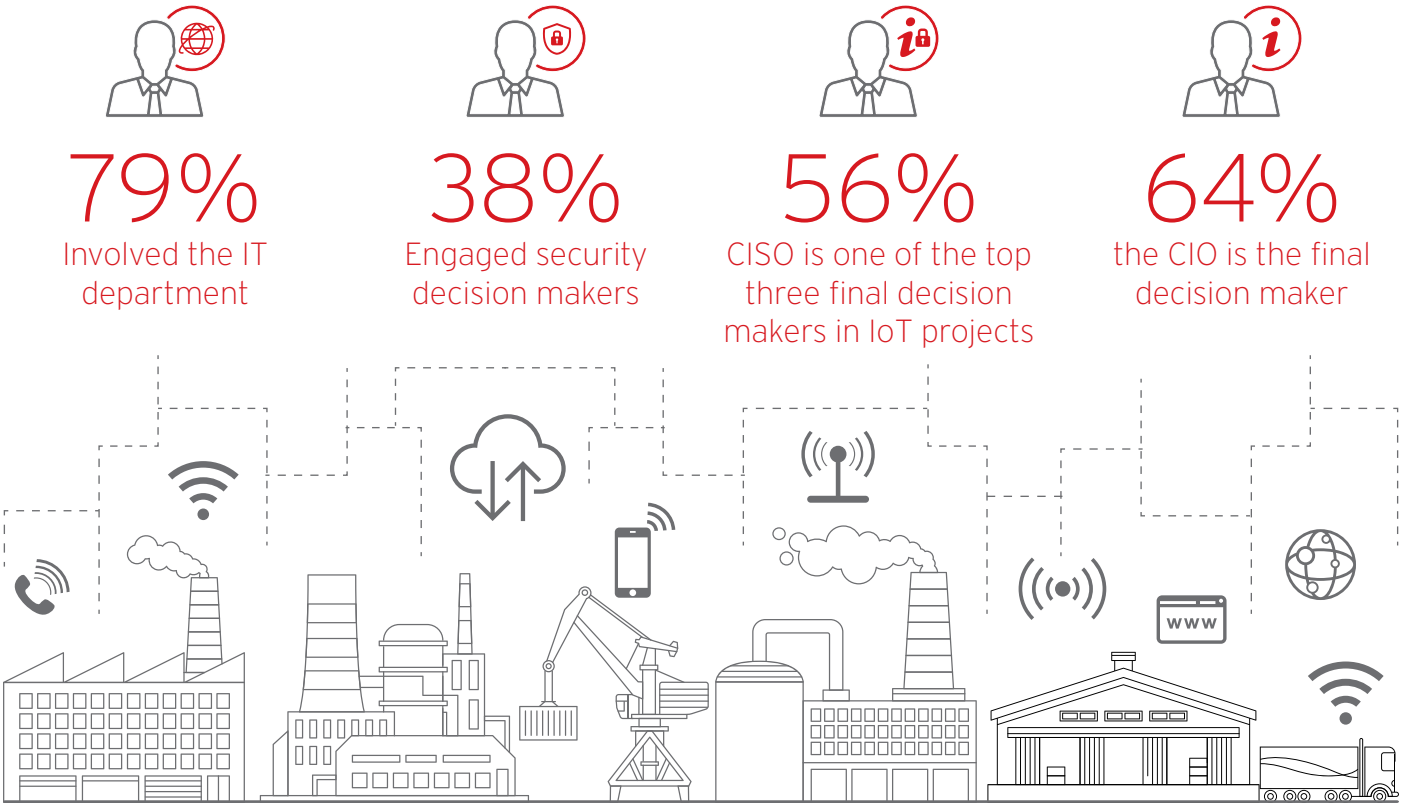


It's clear that global organisations are losing no time in getting started with IoT projects. Industrial IoT was the most popular type, with 62% having already begun implementation, followed by wearables (53%), smart utilities (48%) and smart factory (41%) initiatives. On average, IoT spending is set to rise from $2.51m to an anticipated $2.53m over the coming year. And they're already reaping the rewards. Nearly all respondents (99%) claimed to have seen benefits including quicker access to data (51%), increased customer satisfaction (41%), and cost savings/increased efficiencies (40%).

IoT security: challenges and impacts

However, when we asked IT leaders about the challenges of IoT projects, cybersecurity loomed large. Aside from the key issues of cost and IT complexity (both 40%), came increased security complexity (36%), data security (34%), device security (27%), difficulty in complying with security regulations (26%), and network security (23%), among many others. The vast majority (97%) of respondents also viewed security deficiencies as a potential threat to critical infrastructure, in terms of the complexity of infrastructure (44%), the increased number of endpoints that need securing (42%), and lack of adequate security controls (38%), among other factors.

They're also acutely aware of the potential impact of a major IoT-related security breach, although perhaps not yet in great enough numbers: just 36% recognised it could be very damaging/catastrophic to their organisation. Loss of customer trust (52%), money (49%) and reputation (38%) were the key knock-on impacts feared by respondents. In fact, they're all inter-related: a major breach of data or system outage is likely to hit the brand, which can trigger customer attrition and result in lower profits – a vicious cycle which can be hard for firms to break free from.



Industrial IoT (IIoT) initiatives

Security shunned

Despite the clearly perceived risks, few organisations involve security teams in projects from the start. Of those that had begun IoT initiatives in industrial IoT (IIoT), for example, 79% involved the IT department but less than two-fifths (38%) engaged security decision makers. Similarly, only a little over half of respondents (56%) said the CISO is one of the top three final decision makers in IoT projects, while 64% chose the CIO. The GDPR mandates "data protection by design and by default," so any IoT system that could potentially give attackers access to data must include the input of key security stakeholders from the very start of the design process, or risk serious fines.

Unfortunately, there's a long way still to go: 42% of respondents claimed security is an afterthought and 86% admitted that awareness on protecting against security against cyber threats must improve. Over a third (37%) said they're not able to define security needs when implementing IoT solutions while nearly 33% claimed it's not always clear who's responsible for IoT security: more signs that organisational siloes and immature corporate security cultures are endangering digital transformation.

[1]Gartner, Security and Engineering – Converging or Colliding? Published 18 June 2018 - ID G00348946

Attacks are real

So what are the genuine rather than perceived risks? Unfortunately, real-world threats are widespread: responding organisations claimed on average to have been hit by three attacks against connected devices over the previous 12 months. Only a quarter (27%) had not seen any. What's more, over half (54%) said they had seen an increase in attacks over the past year. Phishing attacks (56%), credential theft (40%) and trojans (30%) were the most popular type, with office (59%), manufacturing (36%) and supply chain (29%) devices most commonly impacted.

Thanks to stolen credentials or access via vulnerability exploitation, attackers could theoretically sabotage critical infrastructure, infiltrate corporate networks to steal sensitive data or even hijack IoT endpoints for use in botnets to launch DDoS attacks, mine crypto currency, and carry out other nefarious activity. The FBI recently warned about such attempts in the consumer and small business sphere.

Conclusion: heading towards a more secure future

IoT systems are already changing the way businesses operate for the better. But with many more global initiatives planned, it's somewhat alarming to find that organisations aren't doing more to mitigate security risks. Although they understand the potentially major financial and reputational impacts of an IoT-related data breach or service outage, few are getting security decision makers involved early enough in projects. Part of the reason may be that there's often confusion about who is responsible for security.

On the plus side, the vast majority admit that cybersecurity awareness needs to increase. So with attacks on the rise, what can the vendor community do? Organisations are looking most for continuous monitoring of unusual communication (56%) and process/system behaviour (51%), centralised threat and vulnerability management information (51%), and virtual patching (41%).

56% Organisations are looking most for continuous monitoring of unusual communication

This is a start, but the IoT ecosystem offers multiple avenues of attack and in the end, we'll all have to do our bit, including IT security teams, vendors and manufacturers.

United Kingdom

Spending on IoT projects in the UK is actually forecast to fall from $2.5m last year to $2.3m in the coming 12 months: perhaps a reflection of continued economic uncertainty. Companies here did quite well in getting security teams involved in choosing IIoT solutions (42%) and at knowing who's responsible for security (76%). More respondents than in any other country felt an IoT breach could be very damaging or catastrophic (46%), and they take customer trust more seriously than any other country (58%). UK organisations are also good at defining their IoT security needs (64%).

On average, UK organisations have been attacked three times in the past year, but are least likely globally to be hit by credential theft (32%) or trojans (24%). Respondents are more likely than their global peers to seek out IoT security offering permanent monitoring of communications (60%).

United States

US firms are going to invest the most in IoT in the coming 12 months: $2.8m. There's a sizeable minority (42%) of organisations involving security teams early on in IIoT projects, but conversely the largest number globally (72%) who claim they always define their security needs during projects. However, just 34% said the CISO is ultimately responsible for IoT security, among the lowest worldwide.

US firms are most concerned globally about the financial impact of IoT breaches (58%), and they feel the biggest threat to their critical infrastructure is the explosion in IoT endpoints (49%). However, despite suffering an average of three attacks over the past year, they're the least likely globally to believe IoT solutions are a security threat (48%). The largest number of US firms (59%) are looking for centralised dashboard functionality in their IoT solutions.

Japan

Japan spent the least on IoT projects last year ($2.1m) although that figure is rising to $2.4m. Respondents were least likely to involve security in IIoT projects (28%), a figure dropping to just 22% for wearables initiatives. They're also least likely globally to know who's responsible for security (45%) or to place ultimate responsibility for IoT security on the shoulders of the CISO (33%).

Yet the awareness is there: Japanese organisations are most likely to believe IoT is a security threat (74%), having experienced an average of six attacks over the past year – twice the global figure. Attacks are increasing in volume for more organisations here than in any other country (73%). They're also most likely globally to suffer phishing attacks (65%) and attacks targeting office devices (68%).

France

French firms spent the most on IoT last year ($2.8m) but are reining that in next year to $2.5m. Along with Japanese respondents, they're least likely to involve security in IIoT projects (28%) early on, yet conversely they're also least likely to regard IoT security as an afterthought (39%). Having suffered an average of three attacks last year, most are hit via phishing (51%) and credential theft (41%), but they are also the second top country for trojans (36%).

French organisations are also most likely globally to suffer IoT attacks targeting manufacturing devices. To help combat these raids, they want permanent monitoring of system behaviour (53%) in IoT security solutions more than their global counterparts.

Germany

Germany is one of the most mature countries when it comes to IoT security: respondents are most likely (43%) to involve security teams in choosing of IoT projects. They're also most likely (60%) to view the CISO as one of the top three final decision makers when choosing these products. However, conversely, they're most likely to believe there's a need to improve security awareness (91%) and that security is an afterthought (47%). Perhaps they have more rigorous standards than some of their counterparts around the world.

German respondents also downplayed the seriousness of an IoT breach: fewer than in any other country regarded one as potentially very damaging or catastrophic (21%). Perhaps they're more confident in handling such an attack. Real-world attacks last year were the same as the global average (3) but fewer organisations than elsewhere saw attack volumes increasing (42%). German firms are most likely globally to be hit by credential theft (46%) and favour virtual shielding (43%) more than their counterparts.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With more than 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit here

www.trendmicro.com