The IoT "time bomb" report: 49 security experts share their views

We consult a panel of IoT security experts to provide some insight on what businesses need to know.

This is an editorial article by Kathryn Cave, Editor, IDG Connect

Everyone is talking about the Internet of Things (IoT). Connected devises are gaining traction in homes and businesses. The possibilities for what this will mean in our future are endless. And yet it is widely recognised that security is still a massive flaw and exposes a vast surface of things to attack.

But how big a problem is this and what can we do about it? Well, to find out we asked global security experts to get in touch with answers to these four key questions:

1. How big a problem will lack of security on IoT devices be?
2. What do big businesses fail to grasp about this?
3. What can be done to rectify the problem?
4. Anything else you want to add that you don't think gets enough media coverage in this area?

In response we received 50 pages (just under 25,000 words) from 49 different security experts. The short online report below distils the most interesting commentary. As there was some overlap in views this does not include direct quotes from every individual who took part but it does cover the overall message.

Overview

Everyone we spoke to agreed that lack of security on IoT devices is a problem. Naturally, the scale of this depends on industry and the impact of the hack.

The most repeated solution offered was that security needs to be built into devices from the go-get not simply tacked on the top. Yet as with any security problem there was also a lot of talk about soft issues like understanding the risk, managing people and access privileges and making sure that individuals are aware of their own areas of responsibility.

In order to make this vast glut of information as digestible as possible we have broken this down into four simple sections with relevant commentary listed underneath. These are:

1. Some words on the problems
2. Some words of warning
3. Some words of positivity

4. Some words of advice – this includes a five point checklist of minimum security controls

Some words on the problem

The business imperative to move forward
"The problem is the temptation for businesses and the government to surge ahead with new smart grid technology, connecting the internet of things, without adequate protection. [But just] imagine the cost to businesses in London if someone managed to close down part of London Underground for a few hours." *Matt Brake, Business Development Director focused on IoT for Critical Software*

Innovation often takes priority over security
"Unfortunately, the speed with which innovation is happening means that security is often being added as an afterthought rather than being built-in from the start, leaving vulnerabilities for hackers to exploit. This is no small problem." *Sukamal Banerjee the head of HCL Technologies' IoT taskforce*

The threat surface is becoming vast
"Any device that is connected, regardless of whether it's IoT-enabled, is a potential target for a cyber-attack. The devices themselves may not be the end target (they could be used to carry out malicious activity as part of a botnet attack), but they could be used as a gateway into the broader enterprise network and critical systems." *Mary Beth Hall, the Director of Product Management and Development at Verizon*

A fragmented space means the hackers are circling
"It's an incredibly fragmented space and network security has not been a priority for manufacturers, so typical IT-focused security endeavours often don't even register on the radar. IoT is going to be the new honeypot for hackers and you can expect to see a lot of hacking endeavours aimed at it." *Steve Bell, Security Expert at BullGuard*

It is it is impossible to ignore the fact that everything costs money
"Corporate cost control is one of the main reasons for the low quality of many IoT hubs or Wi-Fi routers, resulting in simplified hardware that hinders basic security principals of integrity and failover." *Thomas Fischer, Principal Threat Researcher at Digital Guardian*

There is always a gradual evolution from consumer to enterprise
"While 'things' often begin as consumer commodities, they can evolve into enterprise 'things'—just as mobile technology did. Most IT departments, however, aren't responsible for managing the physical security of these 'things', and this could signal a holistic shift in how all aspects of security are managed within the enterprise." *Martin Borrett, CTO at IBM Security Europe*

Some words of warning

Emerging technology repeats the mistakes of history
"Emerging technologies typically repeat the mistakes of history and it is common to find old flaws in new technologies; particularly security related flaws. The good news is that the security posture of emerging technologies tends to improve over time." *Chris Oakley, Managing Principal Security Consultant at Nettitude*

Our time to learn is shrinking
"While we need time to start to understand the issues, our hyper-connected world means we don't have a lot of time to solve some of these challenges. The window of understanding continues to shrink as technology continues to move faster than ever." *Lawrence Munro, Director of EMEA & APAC at Trustwave*

Some IT staff shrug their shoulders and think, 'our of sight out of mind'
"The inherent problem with security within an IoT eco-system is that the devices are invariably not located within the corporate environment. Many IT staff see incoming data as being securely transmitted and stored within their secure environment but are not looking at the devices themselves. This out of sight, out of mind approach has resulted in a hugely increased attack surface with no clearly accountable individuals owning the problem." *Simon Ratcliffe, Consultant, Advanced 365*

Five core threat parameters
"The areas within the IoT and wearables industry that are most at risk are: security cameras, private photo collections (especially those stored in the cloud), mobile banking and medical records - even doors and automated fences! These should have additional security measures in place to protect against outside threats." *Nazar Tymoshyk is a Security Consultant Lead, R&D, at SoftServe*

Open source NoSQL databases are not commercially viable
"The open source NoSQL databases people are turning to for huge scale IoT applications aren't necessarily ready for commercial applications." Dave McCrory, CTO at Basho

IoT security is way more than just the security of the 'things'
"When people think of the security for IoT, they, understandably and justifiably, think of the security of the devices (the 'things') themselves. Although, this is naturally important, there is another dimension here that is often overlooked. Each of these devices adds risk, complexity, and new behaviours to the environment it finds itself in. Within an organisation, this creates new challenges around security monitoring, security operations, and incident response. It's important to consider how to mitigate these new risks by adjusting the organisation's detection, analysis, and response strategy and capabilities accordingly." *Josh Goldfarb, CTO-Emerging Technologies at FireEye*

Security must be built-in not added on
"Security cannot be an overlay. Development of connected objects needs to be done with scenario planning in mind so that the security mitigation is built-in." *Adrian Crawley, Regional Director for Northern Europe at Radware*

There is a psychological risk in IoT
"Part of the risk is a psychological one. I often call IoT devices, stealthy computers. In part because most people don't think, 'computer' when they look at certain IoT devices. Unfortunately, the result is that people also don't associate the same risk with these devices as they do with computers. Even though the risk profile is much the same." *Corey Nachreiner, CTO at WatchGuard Technologies*

The security gap between the device and the cloud is overlooked
"One of the biggest points that is frequently overlooked is the actual security gaps between the device and the cloud." *Reiner Kappenberger, Global Product Management at HPE Security*

Often the wrong people can access devices
"As the adoption of IoT devices in the workplace continues to rise exponentially, security relating to accessing devices will continue to be front of mind to the IT manager and C-Suite. The biggest threat to any business large or small, is understanding who actually needs access to devices and then knowing who has what level of access to the network." *Stuart Facey, VP International at Bomgar*

Businesses allow off-the-shelf products to make them too comfortable
"I think that, outside of the security team, there is a general feeling amongst CEOs and business leaders that if you've invested in cyber security products then you are pretty much safe. Very few organisations are mentally and financially geared up to support the security team's needs for the constant arms race that cyber security has become." *Bradley Maule-ffinch, Director of Strategy, IP EXPO Europe*

A 'do everything' solution may just do nothing
"We find organisations spend too much on security technology – searching for a cyber cure-all – and as a result are becoming less secure." *Chris Richter, Senior Vice President of Global Security Services at Level 3 Communications*

Your CCTV can go unwatched
"One area which big business has largely ignored and which doesn't get much media coverage is the potential for attacks via CCTV systems. Attacks are usually initiated by computer botnets, but in recent months we have seen major distributed denial-of-service (DDoS) attacks triggered by malicious requests from CCTV cameras [e.g. this one in the US]." *James Wickes, co-founder and CEO, Cloudview*

Don't let yourself be first to be compromised
"Ultimately, the market place will decide what the 'good' (secure) IoT devices are and what IoT devices are 'bad" (insecure). Being first to find out you have a 'bad' device, could be a very expensive situation if it's the reason hackers get into your infrastructure." *Ian Trump, Security Lead at global cloud-based IT service management solutions LOGICnow*

You must decide who is responsible
"I see more and more companies struggling to determine who will be responsible for security as they map out their strategy for adoption and deployment." *Adrian Crawley, Regional Director for Northern Europe at Radware*

All that 'fridge' business has led to flippancy
"In my view there has been too much flippancy in the media about the likes of 'hacking my fridge' which has watered down the potential security awareness and key consumer messages. If a device is connected then criminals may seek to exploit that device as a weak link and as a 'back door' means of accessing far more important credentials and devices." *Brian Kinch, Senior Partner of Client Services at FICO*

The barrier for IoT entry is low
"The barrier for entry into the IoT space is low. Anyone hobbyist, student, or entrepreneur can go online and order all the parts necessary to create their own IoT device. Very few of these people and even organisations have the security expertise to recognise the security flaws in their designs and implementations because that is not the focus, making a selling product is." *Aaron Bryson, Chief Security Architect and Product Security Manager, Kony*

Some words of positivity

Things are not as bad as they seem
"We are actually a little ahead of the game. Right now, it doesn't seem like a majority of attackers is directly targeting this potentially big weakness." *Corey Nachreiner, CTO at WatchGuard Technologies*

Due credit should go to the decent security companies
"In my personal experience, there are some businesses that do give IoT the security diligence it deserves and possess the technical and security expertise to do so. Behind the scenes, they work hard to make sure that they release secure products. I have a lot of respect for those businesses.

"Unfortunately, these kinds of things aren't talked about in the media and businesses aren't transparent about the awesome things they are doing in the security space. A paradigm shift is welcome, where businesses openly talk about how they are securing their IoT and changing the status quo. It sets an example for others to learn from and to aspire to." *Aaron Bryson, Chief Security Architect and Product Security Manager, Kony*

Some words of advice

Know your assets, the threats and their impact
"For businesses using IoT devices, the first step to protect yourself is to be aware of the risks. This means you have to know what your assets are, what your threats are, and what the impact could be. *Tobias Zillner, Senior IS Auditor at Cognosec*

Educate vendors on the build
"The cyber security industry must continue to educate vendors, so that security becomes more 'built in' than 'bolted on'." *Chris Oakley, Managing Principal Security Consultant at Nettitude*

Be aware that IoT is an ecosystem not just a series of devices
"In designing and testing the system, organisations must consider and run scenarios in which devices are compromised. This process ensures that the system is able to identify, isolate, and report the compromised devices while the rest of the system remains operational, avoiding the scenario where an entire network can be downed by a single point of failure." *Martin Borrett, CTO at IBM Security Europe*

Segment networks to limit the damage
"Segment IoT networks and systems to limit the spread and damage of any attack. You don't want a breach of a relatively innocuous sensor to lead to the compromise of your connected device or enterprise systems. Segmentation will also help reduce the amount of sensitive information criminals can exfiltrate." *Josh Bressers, Security Product Manager at Red Hat*

Employ smart gateways
"Rather than placing IoT devices directly onto corporate networks, it will be important to deploy smart gateways to segment and monitor the IoT networks." *Lawrence Munro, Director of EMEA & APAC at Trustwave*

Control your data access is crucial
"For businesses – where the device may be connected to the corporate network and, in

turn, the confidential data held there – they need to closely manage the privileged accounts which control the device." *Matt Middleton-Leal, Regional Director UK & Ireland at CyberArk*

Security features must be included in initial designs
"We need to continue to pressure IoT manufacturers to consider security early in their design, and implement things like secure boot, encryption, strong authentication, and other steps to make our IoT devices more secure out of the box." *Corey Nachreiner, CTO at WatchGuard Technologies*

Devices must be capable of withstanding attack
"The IoT providers themselves need to ensure their devices and solutions are capable of withstanding attacks and that their customers can safely deploy IoT solutions in an assured manner." *Steinthor Bjarnason, Network Security Research Engineer at Arbor Networks, a security division of NetScout.*

End users must accept some responsibility
"Users need to be educated more about the dangers of unsecure IoT devices, as responsibility does not just fall on the shoulders of organisations. Just as a computer or mobile needs a strong password and mindfulness about who has physical access, so too will IoT technology." *Mike Turner, Global Cybersecurity Business Leader at Capgemini*

Remember people are always to blame
"The weakest link is always the staff. Investing in training and awareness is integral and often neglected – however, the employees are usually the first line of defence." *Bradley Maule-ffinch, Director of Strategy, IP EXPO Europe*

Machine learning and data analytics can supply intelligence
"Enterprise leaders should look to how they might use machine learning and big data analytics as part of their plan to more quickly gain insight into potential threats in IoT environments, where networks and network-connected devices will grow at staggering rates." *Mike Stute, Chief Scientist at Masergy*

Five minimum security controls
"While all Internet-connected 'things' are different and require different security, the following controls should be implemented at the very least in order to ensure a more secure IoT:

1. **A secure operating system with trusted firmware guarantees.** This includes the ability to perform over-the-network/over-the-air updates across untrusted connections.
2. **A unique identifier.** While IPv6 is key to identifying 'things' on networks, these "things" also need a subscription to a trusted identity database. Since many 'things' don't directly interact with users like traditional computers, the concept of traditional authentication doesn't apply, particularly when 'things' interact in a machine-to-machine (M2M) environment.
3. **Strong authentication and access control.** When users access the data on 'things' or control them—usually through a cloud service from the user's mobile device—it's crucial to ensure that the user is who he or she claims to be. You wouldn't want a thief to be able to unlock and start your car with a simple username and password, especially considering the recent spate of credential compromises and the knowledge that most users choose simple passwords. In fact, research shows that '123456' and 'password' are still the two most common passwords found on the internet.

4. **Data privacy protection.** The data that flows to and from 'things'—and that may be stored on 'things' or their controlling devices—is often sensitive. Drivers may connect their mobile phones to the in-vehicle infotainment system, which has access to their contact information and, possibly, their email and text messages. With mobile payments starting to appear on new mobile phones, credit card information may be accessible to the vehicle. Credentials to access home automation and industrial control systems can also be exposed if not properly protected. Often, the solution to the issue of privacy is data and transmission encryption.
5. **Strong application security.** Vulnerabilities arise due to software bugs. Hardware manufacturers are often not experts in software development, including web applications that may reside on the 'thing', or exist as a cloud portal and mobile apps. Security vulnerabilities are legion and often catastrophic, as evidenced by the recent Heartbleed OpenSSL vulnerability and the even more recent Bash Shellshock vulnerability. Manufacturers of 'things' are coming up with new product ideas every day and may rush their products to market without implementing a security development lifecycle or conducting thorough security and functional testing."

   Martin Borrett, CTO at IBM Security Europe