Securing Smart Devices
New consumer expectations for the Internet of Things
Securing Smart Devices

It’s no secret that smart products are becoming an increasingly common part of consumers’ lives. The convenience and efficiency they offer is incredibly attractive to busy people looking to save time and make their lives easier. This is reflected in the smart product market, which is already immense and growing rapidly – $235 billion USD worth of connected devices were sold in 2017 and annual sales are expected to reach $520 billion by 2021.¹

Given this incredible market growth, manufacturers are eagerly responding by developing new smart products at breakneck speed. However, because many connected device manufacturers don’t consider their products to be targets for bad actors, many smart devices are shipped with built-in vulnerabilities that leave the product, consumer, and manufacturer at risk.

The reality for smart device manufacturers is that any connected device – even smart light bulbs – can become a target for bad actors. Whether hackers choose to hijack devices and hold them for ransom, or leverage thousands of unsecured connected devices in a large-scale botnet attack such as Mirai, the takeaway is the same: if a device connects to the internet, it’s at risk. By 2020, it’s estimated that 25% of cyberattacks will target Internet of Things (IoT) devices.²

With the average data breach costing a business more than $3.8 million globally and $7.9 million in the US,³ manufacturers are risking their reputation and bottom line by shipping unsecured products. And the costs don’t stop once a breach is contained – after the dust has settled, brands have to consider possible litigation, clean-up costs, reparations, or even retroactive fines from regulators.

EMPOWERING MANUFACTURERS WITH NEW CONSUMER INSIGHTS

These days, with new threats and cyberattacks cropping up daily, a brand’s reputation matters more than ever. With consumer perspectives changing so quickly, it’s vital for manufacturers to keep a finger constantly on the consumer pulse. To better understand how the allure of connected devices stacks up against growing security concerns, Microsoft commissioned Greenberg Strategy to conduct an in-depth study of the topic. We interviewed and polled thousands of consumers across the US, UK, and Germany, collecting both qualitative and quantitative data about how customers view smart devices.

In this white paper, we’ll discuss our findings and what they mean for device manufacturers. Our goal is to empower manufacturers with insights that help them take advantage of market opportunity, while protecting their brand from risk and addressing consumer security concerns.

BY 2020, IT’S ESTIMATED THAT 25% OF CYBERATTACKS WILL TARGET INTERNET OF THINGS DEVICES
CONSUMERS ARE GROWING MORE ATTUNED TO SMART DEVICE RISKS
As consumers learn about smart devices and their potential security vulnerabilities, our research found they’re becoming more cautious. When connected devices first landed on the market, their novelty and convenience outweighed consumer desire for security. A 2016 consumer survey found that only 31% of consumers updated their smart devices as soon as possible and 40% of consumers had never intentionally updated their devices. However, this initial disregard towards security seems to be shifting. For instance, many eyes were opened when the Mirai botnet attack took control of thousands of smart devices by scanning the internet for open Telnet ports and logging in with default passwords set by manufacturers. Using simple source code that’s now publicly available on the internet, bad actors were able to amass an army of smart devices to carry out various cyber-attacks while concealing their location, identity, and intentions.

Consumers are also realizing their unsecured smart products aren’t only at risk of becoming cyber-weapons for hackers, but can just as easily be used to expose private information. One 2018 report found that by infiltrating an IoT security camera and daisy-chaining additional IoT vulnerabilities, hackers were able to breach a secure network and access private data without ever touching a traditional computer.

Reports like these are resonating with consumers, prompting concerns around societal and personal safety. From a societal standpoint, our research found 87% of consumers were concerned about their device being used to harm others, with nearly 30% citing fears of corporate data misuse, government spying, or general privacy violations. On an individual level, we found 52% of consumers fear a personal data breach and 19% worry that their physical safety could be compromised by an IoT hack, such as a bad actor gaining unlawful

“I’VE REALLY GOT A LIMITED DEGREE OF WHAT I CAN DO. I WOULD SAY THE MANUFACTURER IS THE MAIN PERSON RESPONSIBLE.”

NINE-IN-TEN PEOPLE AGREE THAT MANUFACTURERS SHOULD TAKE MORE STEPS TO SECURE SMART DEVICES

“...I would say the manufacturer is the main person responsible.”
access to their home or smart camera. Surprisingly, this heightened awareness isn’t significantly altering consumer behavior. Despite recognizing the risks, the majority of consumers don’t understand how to protect their devices, or they assume they’re already secure. Our research showed only one out of every three consumers actively takes steps to secure their smart devices, such as updating device software and investing in anti-virus protection. While these measures are helpful, they’re not comprehensive. Much of the security required for smart products is controlled by the manufacturer. End users have no power over what happens at the hardware level, for example, and often cannot adjust default passwords set by the manufacturer. Since there are limited actions consumers can take, they ultimately expect manufacturers to be responsible for device security. Our research revealed that nine in ten people agree manufacturers should take more steps to secure smart devices, with one participant adding, “I would say the manufacturer [is responsible for security] because I think they’ve got a bit more power than I have... I’ve really got a limited degree of [control over] what I can do.” The conclusion here is simple – consumers are calling on manufacturers to provide more comprehensive device security, and if manufacturers want to continue capitalizing on this rapidly growing market, they must deliver it.

**EXPECTATIONS ARE INCREASING FOR SMART DEVICE MANUFACTURERS**

Given this new understanding of consumer perceptions towards IoT security, there are a number of takeaways for manufacturers. In this section we’ll present three key implications from our findings.

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>21%</td>
</tr>
<tr>
<td>Value for money</td>
<td>20%</td>
</tr>
<tr>
<td>Ease of use</td>
<td>11%</td>
</tr>
<tr>
<td>Trusted brand</td>
<td>9%</td>
</tr>
<tr>
<td>Ease of set up</td>
<td>7%</td>
</tr>
</tbody>
</table>

SECURITY IS THE TOP CONSIDERATION ACROSS ALL MARKETS IN THE PURCHASE OF A NEW SMART DEVICE
1. Manufacturers Must Make IoT Security a Top Priority

In order to prevent IoT intrusions and maintain consumer trust, manufacturers must change their approach to connected device security. If they don’t, they may be one high-profile cyberattack away from damaging their brand. Susanne Spaulding, a senior advisor at the Center for Strategic and International Studies, echoed this sentiment at CES 2019: “If we don’t achieve and maintain the trust of potential consumers, clients, and regulators around these devices, we won’t be able to enjoy the benefit that a networked world can offer us.”

Protecting brand reputation isn’t the only reason smart product manufacturers should think differently about security. They must also consider the long-term costs of updating unsecured products, such as hiring security consultants to contain a breach, retroactively building out infrastructure to support remote security updates, and pulling developers off new products to patch older models. For example, imagine a manufacturer who ships device 1.0 today and device 2.0 a year later. As they’re designing 3.0, they realize 1.0 has a known vulnerability and requires an update. Unfortunately, because 1.0 wasn’t built with the proper infrastructure for remote software updates, the team must halt work on 3.0 and return to 1.0. Not only will addressing this problem be an expensive engineering endeavor, it could also impact revenue for 3.0 and potentially cause the manufacturer to miss important milestones like peak shopping times. If devices aren’t built with security updates in mind, manufacturers are liable to face cost overruns when addressing vulnerabilities later.

While the threat of incurring additional costs is a valid motivator for manufactures to bolster security, manufacturers also have an obligation to society. Our research showed people want to know they’re being protected when they open up their personal lives and spaces to smart experiences and new technologies. As a result, it’s vital these experiences are safe for users and don’t put their
wellbeing or data at risk. At the end of the day, manufacturers need to prove consumer trust hasn’t been misplaced by delivering secure devices.

Importantly, this applies to all IoT manufacturers, not just those who build products that perform dangerous or mission-critical jobs like vehicles. Even for manufacturers specializing in seemingly harmless devices like smart light bulbs and cameras, security must be a priority. If manufacturers continue to treat security as an afterthought, customers could be at risk of bad actors holding their devices ransom or “bricking” them.

While this may sound far-fetched, these scenarios are no longer hypothetical. In 2017, a hacker infiltrated a casino’s network via a smart-thermometer located in one of its fish tanks. After infiltrating the thermometer, the hacker was able to navigate into other areas of the casino’s network and eventually export 10 GB of private data to a device in Finland.13 This story and countless others demonstrate that there are no innocuous IoT devices, so all must be properly secured.

With increasing consumer expectations in mind, it’s time to redefine “smart.” Yes, smart experiences are intuitive, insightful, and easy to use, but one more qualifier must be added: secure. If a device isn’t secure, it’s not smart. Embracing this new paradigm will require manufacturers to take a close look at their security posture and make an intentional shift.

2. An End-To-End Approach Is Needed to Ensure Security at Every Layer

Another important conclusion drawn from our research is that the most effective way for manufacturers to prevent future intrusions is by adopting an end-to-end security approach. To reduce risk and address consumer concerns, manufacturers must build products with security in mind throughout the entire design, production, and maintenance process, rather than including security as an add-on. This new approach starts with executive leader-
ship recognizing that exposing customers to risk is unacceptable and making a commitment to prioritize security. Executives who neglect to make security a priority aren’t only risking customer safety, they’re also risking their personal reputation – no one wants to be known as the person responsible for an embarrassing security breach. With executive championship, a security-first mandate has the freedom to flow down the chain to the product designers and owners responsible for building connected devices.

From there, holistic security begins at the hardware level. Hardware is far more expensive to update than other solution components like the operating system and security service, so it’s important to get it right the first time. If the foundation of a device is unsecured, the device itself will always be put in place at the software level and in the cloud. Since hackers will always target the weak point of a device or system, it’s imperative all security layers work together seamlessly and without fail. With better peace of mind that comes from built-in, end-to-end security, businesses can spend more time focusing on strategic initiatives that deliver value to their customers.

Additionally, rigorous attention to security shouldn’t cease after the product is finished and released. With many other products, the seller-buyer relationship ends at point of purchase, but with smart devices, the relationship is ongoing. Because security evolves so rapidly, a highly secure device that’s shipped today may become unsecure tomorrow. As time goes by, new hacking techniques and the ability to crack ciphers with increased processing power will require devices to be monitored and updated.\textsuperscript{14} Our survey also underscored this point – 90% of participants believed that any piece of smart tech can be hacked.\textsuperscript{15} If manufacturers don’t maintain constant vigilance, they allow their products to become progressively easier targets.

Even after connected devices reach the end of their lives and are thrown away, their data still need to be secured. A recent study into discarded smart bulbs found none of the brands examined did anything to encrypt the data housed in their bulbs. This meant anyone could grab a bulb out of the trash or an outdoor fixture and easily extract

**OUR RESEARCH FOUND 86% OF CONSUMERS WOULD BE WILLING TO PAY MORE FOR A DEVICE WITH BUILT-IN SECURITY**
information about the owner’s network, including their Wi-Fi password.\textsuperscript{16} This should be a wake-up call for all smart product manufacturers – not only must you secure your devices while they’re active, their data must be permanently encrypted once the device is disconnected.

By securing their devices from the silicon to the cloud, manufacturers can significantly improve physical product security and proactively increase their options for future updates, ensuring swift response to emerging threats or new government mandates.

3. Regulators May Soon Make Device Security a Requirement, Not a Request
Consumer aren’t the only ones putting pressure on manufacturers to improve device security. Many governments already consider ineffective IoT security a threat to critical infrastructure, and they’re right to be concerned – our research found 81% of renters or homeowners already own a smart device in their home.\textsuperscript{17} If compromised, the sheer volume of these devices could create a significant attack surface. As such, regulatory bodies around the world are developing more stringent smart product security rules and some are already taking steps to enforce them.

In 2017, the United States Senate introduced the Internet of Things Cybersecurity Improvement Act, which was later referred to the Committee on Homeland Security and Governmental Affairs. The state of California recently passed the first significant piece of legislation, with SB 327, which mandates that all connected device manufacturers equip their products with reasonable security features starting in 2020.

In 2018, the Department for Digital, Culture, Media & Sport in the United Kingdom published

\textit{“WE MUST REDUCE THE BURDEN ON END USERS BY EMBEDDING EFFECTIVE CYBER SECURITY PRACTICES AT EVERY STAGE”} 
\textbf{MARGOT JAMES, UK MINISTER FOR DIGITAL AND CREATIVE INDUSTRIES}

\textbf{Secure by Design}, a 37-page report intended as a security code of practice for smart device manufacturers.\textsuperscript{18} The report specifically urged manufacturers to update their approach to security, with Minister for Digital and Creative Industries, Margot James, stating: “As government and industry work together to ensure we protect the UK from cyberattacks, we must also reduce the burden on end users by embedding effective cyber security practices at every stage of a connected
And in Asia, Japan is taking a unique approach to smart product security. To mitigate security concerns leading up to the 2020 Summer Olympics in Tokyo, the National Institute of Information and Communications Technology (NICT) is orchestrating a government-led attempt to hack citizens’ IoT devices and compile a list of those at risk.20

As governments and consumers place increasing emphasis on IoT security, forward-thinking manufacturers should be paying attention if they want to avoid expensive recalls. These implications speak volumes, and manufacturers who give them careful consideration and secure their devices from end-to-end will not only enjoy added benefits but establish themselves as a brand of choice in a crowded market.

NOW IS THE TIME TO BECOME A TRUSTED SECURITY LEADER
We recognize there are many variables that manufacturers must balance when making changes to their existing strategies, and cost containment is likely top of mind. However, when IoT security is viewed not as a technology cost, but as an investment in a brand’s future, the benefits of end-to-end security quickly become apparent. Let’s take a look at a few of them.

1. Reducing Risk and Protecting Brand Trust
First, as mentioned earlier, all it takes to damage a brand’s reputation is one high-profile cyberattack. While consumers may not remember every brand’s missteps, our research found they rely heavily on third-party sources to evaluate the devices they’re considering for purchase. Third-party sources have much longer memories and are likely to surface security concerns with a given company or product, impacting consumer purchasing decisions. In our research, 65% of people stated they wouldn’t purchase a smart product from a brand that has experienced a security breach.21 By delivering on a promise to enhance device security, manufacturers can ensure their brand remains strong and continue to grow their influence while mitigating risk at the same time.

2. Securing a Competitive Advantage
Next, companies that accept responsibility for providing better security today will create a distinct advantage for themselves as a trusted brand shaping the future of IoT. By building reputations as security leaders, manufacturers can increase their market share in the years to come. Our research showed 81% of consumers agree that purchasing from a trusted manufacturer is key to improving smart device security.22 And when selecting
a new smart device, security was the primary consideration for consumers globally – 21% cited security as their top concern over value for money (20%).23 One participant commented, “If you put together a smart refrigerator that’s always getting hacked, nobody will buy it and that company won’t make money...If a product isn’t safe the public will go to the next product.”24 As this sentiment deepens and consumers put their wallet share behind trusted brands, competitors with sub-par security won’t be able to measure up.

3. Driving Revenue
Finally, not only are consumers more likely to purchase secure devices, they’re willing to pay more for the added peace of mind. Our research found 86% of consumers would be willing to pay more for a device with built-in security25 and this trend extends to enterprise customers as well. Bain & Company found 93% of executives would be prepared to pay an extra 22% for smart products with better security.26 Bolstering security for connected devices has the potential to drive revenue in two ways. As manufacturers address consumer security concerns, they’ll simultaneously attract consumers from their less-secure competitors, as well as pull new customers into the purchasing cycle who didn’t buy previously due to security vulnerabilities. With new market opportunities available for trusted brands, it’s easy to see how the right investments in IoT security could deliver a lucrative return.

CONCLUSION
Though IoT offers consumers a host of new experiences, smart products also pose significant security risks to society, critical infrastructure, and even individuals. When manufacturers fail to continuously secure their devices, they compromise consumer data and safety, as well as their own reputation and brand – even years after launch.

THE RESULTS ARE CLEAR: CONSUMERS EXPECT DEVICE MANUFACTURERS TO TAKE SECURITY SERIOUSLY

Our research provides insightful snapshots of a rapidly shifting market and the results are clear: consumers expect device manufacturers to take security seriously. Only manufacturers have the power to holistically secure devices from product inception through end-of-life. While adopting an end-to-end security approach for smart products will require investment, the potential to gain market share, add new revenue, and protect customers is well worth the effort. ■
METHODOLOGY
Securing Smart Devices is a Greenberg Strategy white paper, sponsored by Microsoft. Greenberg Strategy performed the research and wrote the report independently. The findings and views expressed in this report are those of Greenberg Strategy and don’t necessarily reflect the views of the sponsor.

Study 1: Greenberg Strategy, "Smart Home Security Qualitative Research Report," July 31, 2018
Eleven focus groups with tech forward, tech laggard and security centric audiences conducted in Chicago, US; London, UK; and Frankfurt, Germany.

Study 2: Greenberg Strategy, "Smart Home Security Flash Poll," September 2018
Online survey conducted between August 28–September 7, 2018 with homeowners or renters of ages 18–65. Total N = 3,005 (US 1,013; UK 1,029; Germany 1,023). Age and gender balanced to census proportions.

Study 3: Greenberg Strategy, "Smart Home Security Quantitative Study," October 2018
Online survey conducted between September 24–October 3, 2018 with homeowners or renters of ages 18–65 considering a smart device purchase. Total N = 3,005 (US 1,000; UK 1,005; Germany 1,000). Age and gender balanced to census proportions.

FOOTNOTES
4 https://blog.ubuntu.com/2016/12/15/research-consumers-are-terrible-at-updating-their-connected-devices
6 https://www.wired.com/story/elaborate-hack-shows-damage-iot-bugs-can-do/
7 Greenberg Strategy, Smart Home Security Flash Poll, September 2018
8 ibid
9 ibid
10 ibid
11 Greenberg Strategy, "Smart Home Security Qualitative Research Report", July 31, 2018
14 https://semiengineering.com/how-to-secure-the-network-edge/
15 Greenberg Strategy, Smart Home Security Flash Poll, September 2018
17 Greenberg Strategy, Smart Home Security Flash Poll, September 2018
18 https://www.gov.uk/government/publications/secure-by-design
21 Greenberg Strategy, Smart Home Security Flash Poll, September 2018
22 ibid
23 ibid
24 Greenberg Strategy, "Smart Home Security Qualitative Research Report, July 31, 2018
25 Greenberg Strategy, Smart Home Security Flash Poll, September 2018
27 Greenberg Strategy, "Smart Home Security Quantitative Study", October 2018