Potential National Security Threat Created by Cyber Attackers Infiltrating Unsecured Smarthome Devices

Clayton Wilkinson

Spring 2019
Potential National Security Threat Created by Cyber Attackers Infiltrating Unsecured Smarthome Devices

Clayton Wilkinson
April 2019

Executive Summary

To combat the potential effects of malicious cyber intrusions and attacks on unsecured home devices, individuals must identify and understand the security risks of smarthome devices and the Internet of Things (IoT), and must implement security protocols necessary to ensure their homes are safe and secure. The failure to do so holds consequences not only for individuals, but in a widely networked society also increasingly carries national security repercussions.

Future national security cyber threats that may start at the individual level and reach the systemic level require looking as closely as the smarthome components within private American homes. Malicious attacks on smarthome devices may credibly come from nation-states and non-state actors, terrorists and extremist groups, transnational criminal organizations and hacktivists who see smarthome components as unsecured gateways and through the IoT infiltrate and terrorize individuals, stealing their financial, medical, and proprietary data. Individuals must perform a risk analysis and understand that due to the broad connectivity of the IoT, one small break in the network can allow adversaries access to the networked system as a whole, leaving individuals vulnerable as well as creating threats to national security interests in some systems.

This research report will discuss the unseen adversaries assessing ordinary smarthome components and whether the vulnerabilities in trusted devices make their owners an easy cyber target. With awareness of these vulnerabilities in mind, the report then offers a discussion on risk analysis and the decisions owners need to make regarding trade-offs for security versus convenience; evaluating the personal risk and ultimate impact to their lives. It will also look at the vulnerabilities in internet routers and consider how artificial intelligence-powered technology is producing tools that can be used to take control of smarthome components, spread malware, and execute distributed denial of services attacks.

To safeguard against the personal and systemic security disruptions that may be incurred by smarthome vulnerabilities, careful consideration of resilience—the ability to withstand an attack and restore service—will be reviewed as well as the possibilities and tools for individuals, communities, and businesses to shore up defenses against future attacks. Past dismissive or neglectful attitudes toward smarthome and networked device security can no longer continue without risking escalating costs, related to the vulnerabilities of these systems, that are likely to far outweigh short-term gains in convenience.
Unseen Enemies Accessing Smarthome Components, Making Americans Easy Cybertargets

America is currently experiencing a cyber war with unseen adversaries attacking trusted personal smarthome components. US citizens are increasing their purchase and use of internet-connected devices without a commensurate investment in personal security protections, resulting in a dangerously rich target set for cyber criminals, terrorists, extremist groups, transnational criminal organizations, sophisticated state actors, and hacktivists, each with malicious intent to obtain power, finances, and/or prestige.

In the spring of 2018, the US along with United Kingdom issued a first-of-its-kind joint warning about Russian cyberattacks that could infiltrate individual homes, and stated that the exploitation would be due to the increasing popularity of internet devices around homes and businesses. Yet despite government warnings and media coverage of this and other types of cyber threats, US citizens’ tendency to buy the “latest and greatest” internet-linked smarthome components continues to grow. Total sales of internet-connected devices are exploding, with expectations of 200 billion connected devices by the year 2020, which averages 25 connected devices per 100 inhabitants in the US. Individual buying trends are illustrated by Amazon’s Echo and Google’s home device sales being up by 137% to 19.7 million units in the 3rd quarter of 2018. The potential for cyber criminals to use these smarthome devices as a way to steal credit card data, personally identifiable information, or intellectual property, is high. The vulnerability of financial information is a major concern, with 81% of personal financial advisors saying cybersecurity is a high priority for protecting personal financial assets, yet only 29% feel their clients are prepared. This is illustrated by the interconnection of smarthome devices with personal bank accounts, many having a direct link allowing individuals to make purchases and pay bills online, resulting in financial data being at high risk to be accessed through these devices.

People mistakenly stereotype cyber criminals for going after governments or large business entities, but the reality is they often go after those most unprepared—and the Internet of Things (IoT) in personal households, which includes smarthome components, is seen as an easy target. As people continue to purchase internet-connected devices without installing necessary security protocols, updating firmware, and using adequate password protection, this equates to inviting their enemies into their homes.

The East Coast Polytechnic University found that individuals may not even know they have been attacked; cyber invaders can remain dormant waiting for specific timing to gain their objectives. Estimates are that 40% of smarthome appliances are targeted by botnets and this number will increase to 75% by 2021. With the use of artificial intelligence-powered cyber tools and the use of botnets, which seek out interconnected devices including routers, cameras, refrigerators and even thermostats, cyber criminals can infect personal systems with spam and engage in distributed denial of services (DDoS) attacks—an attack in which multiple compromised computer systems hit a target by flooding the targeted devices with incoming messages, thus causing the system to slow, shut down, or crash. An extreme number of connection requests or packets containing malware are used to overwhelm the system. In 2016 DDoS attacks were used to shut down the internet for millions of people in the US, and investigations showed that a large scale botnet was to blame, which infected 100,000 devices. Dr. Eric Hawley, the CIO of Utah State University, feels that DDoS is the biggest threat of IoT at a
national level. He stated that businesses who distribute smarthome devices cannot rely on customers to understand the high vulnerability and existing threats that come with evolving technology, which should be leading them to take security actions. Because of consumers’ unwillingness to keep their equipment updated and secure, he believed that in the future we may actually see insurance claims due to use and misuse of smarthome devices. He stated that his concern with the IoT is with those individuals whose routers were not secure, which could allow DDoS attacks to local financial institutions, shutting down systems for all within a community, due to the interconnected nature of the network.\textsuperscript{11}

As discussed above, most smarthome components have little to no built-in security. Home routers and security cameras are top on the list for attacks because of their lack of built-in security. Furthermore, few of these devices have mechanisms to update software, creating future risk. Many of these devices have default hardcoded passwords which hackers can exploit.\textsuperscript{12}

Dr. Jacob Gunther, department head of the Electrical and Computer Engineering Department at Utah State University, worked and developed smarthome devices from 1998 to 2000 and stated that during that time there was no security on devices and that security was not even a consideration. He pointed out that if a device is activated and has power to the circuits (i.e. all electronic devices), there is a risk of hacking and that even unplugging the unit might not provide security. Dr. Gunther was also concerned about socioeconomics relating to smarthome components, and stated that cyber criminals will go after and hack the weakest links, thus making low socioeconomic strata families especially vulnerable to these kinds of attacks—as they are usually the owners of cheaper products. He displayed three units capable of spoofing AM, FM, and GPS signals and interfering with wireless systems which were small and readily available; one device was actually given to him by the manufacturer, to help teach students (the manufacturer hoped that the students would buy them for themselves). The only limiting factor to the device’s capability was power to the unit, which controls the range of effect. The best unit Dr. Gunther had could attack devices within a 1000 meter radius, using only the power equal to that of a laptop battery transferred through a USB cable, or less than the power of a standard 60 watt household light bulb.\textsuperscript{13} The ease with which these attacks can happen will only increase if proper defensive actions are not taken.

Citizens need to educate themselves to recognize the personal threats internet connectivity brings versus the tradeoff of convenience. With this in mind, individual consumers may not know how to fully evaluate their personal risk. Dr. Peter Tippett lectures on the use of “The Risk Equation”, which can be illustrated as Personal Risk = Threat x Vulnerability x Impact.\textsuperscript{14} This equation is ideal for a consumer to determine their comfort level in utilizing smarthome components. In previous sections, it has been established that there is a threat prevalent against those things connected to the internet. Vulnerability ideally would be minimized, as part of the individual analysis and this portion of the equation is what an individual has the most control over, as individuals can establish a level of defense of their choice. Impact is often the hardest to evaluate; this is the point where the concept of resilience comes into play, requiring evaluation of the effectiveness of the current defenses, and how fast service/security is regained after the attack. Usually impact also comes with a financial cost. Ignoring threats and vulnerability in defenses will lead to the impact being high, but if the resulting impact has little overall value to
the individual, little to no cost should be deployed to mitigate the impact. Peter Tippets’ risk
equation of determining threat, vulnerabilities, and impact relationships needs to become a
normal part of individuals’ lives.

Another reason that individuals must take personal responsibility to secure their
smarthome components against the enemies attacking their homes is because government
protocols will have minimal effect. While government entities, currently with the Department of
Homeland Security at the head,\textsuperscript{15} can establish policies and procedures and encourage education
on security protocols, at best they are being responsive to threats, rather than anticipating
threats. The Federal Trade Commission\textsuperscript{16} and others tasked with cybersecurity are reluctant to
force best practices on manufacturers, as they are unclear on how to enforce personal home
security measures. The fast paced technology advancement and growing number of smarthome
devices have caused government entities to be reactive rather than proactive in dealing with
legislation, codes and enforcement. There is a hope that public awareness will engage to mitigate
the need for regulation. The government has been reluctant to instigate hard legislation for fear
that innovation would be crippled.\textsuperscript{17} Knowing that only the marketplace will drive corrective
measures, customers need to insist on built-in security measures in smarthome devices.
Distributors of these devices would have to make changes to continue to have customer buy-in,
ensuring their business profitability. Individual customers should require that components
include instructions and provide tutorials and explanations of security protocols, to protect
individuals’ data, as well future firmware updates. But even with these proactive steps, the
greatest risk to most networks is router vulnerability.

\textit{Vulnerability in Routers Allow Nation-States and Criminals to Hack Proprietary Information}

Cyber attackers can take advantage of personal router vulnerabilities to commit nefarious
acts, mostly due to owners’ limited implementation of security protocols and procedures,
resulting in owners’ finances, access to passwords, and health and personal identity information
being stolen. This point of vulnerability in most American homes can be taken advantage of to
seriously compromise an individual’s data. Routers are the most frequently exploited type of
device; in 2017 these attacks made up 33.6\% of Internet of Things attacks. This represents a 600\%
increase of IoT attacks in 2017.\textsuperscript{18} The high cost incurred after the attacks does not only affect the
individual, but in the most coordinated and severe cases could go from node to node, bypassing
any secure node and cascading through the network as a whole due to the interconnectedness
of devices, creating a potential national security crisis with significant negative impact to the
economic health of the US.\textsuperscript{19}

The American Consumer Institute (ACI) conducted research showing that currently in US
homes and offices five out of every six (83\%) Wi-Fi routers are at risk of cyberattacks because
their firmware is inadequately updated for security vulnerabilities.\textsuperscript{20} Additionally, in May 2017
Russian-linked botnets attacked 500,000 vulnerable home and office routers and network-access
storage (NAS), located in 54 countries. The takeover granted hackers control over the infected
devices, including deactivation and taking them offline. The malware that was transmitted also
allowed hackers to compromise user data. The FBI intervened, recommending rebooting all
devices, updating firmware, and installing security patches.\textsuperscript{21}
While there is a known threat to and vulnerability within personal routers, the Department of Homeland Security along with the support of other government entities can only do so much in protecting sensitive information without the concerted effort of the private sector, which are those entities in the national economy not under direct government control. Private manufacturers and distributors of IoT devices do not monitor attacks after the routers have been sold. Most if not all routing devices, which are central to the networking process, come with administrative passwords that allow for product use, but provide no real security. Attackers first attempt to use these standard admin passwords to gain access, and if any one of the interconnected devices is breached, all devices are at risk of exploitation. Consumers need to recognize that even if they purchase the most advanced technological routers, if they are dismissive in setting up and using security, the device itself will not protect them.\(^{22}\)

If current trends of consumer dismissiveness regarding router security hold true, exposure to risk will continue to be underrated and the financial cost will continue to grow exponentially. Router attacks compose part of the enormous bill associated with cyberattacks nationwide, with the Council of Economic Advisors reporting that malicious cyber activity in US cost between $57 billion and $109 billion in 2016.\(^ {23}\) It is projected that cyber-crime will cost the world in excess of $6 trillion annually by 2021, making it more profitable than the global trade of all major illegal drugs combined.\(^ {24}\)

Homeland Security acknowledges that mitigation of malicious cyber activity is complex and there is no single solution.\(^ {25}\) While routers are the gatekeepers to many smarthome components, continued proactive actions by both public and private sectors are necessary to combat the continual rise of cyber-crime. DHS should continue to sponsor public awareness campaigns and reporting systems to accumulate data. Their top priority should be to institute regulations for the manufacturing of routers, requiring security features protecting against cyber-attacks with updateable firmware. Wi-Fi router service providers should ensure contractual relationships between sellers and buyers including updated security controls, monitoring and logging of client systems regarding suspected security events.\(^ {26}\) Finally, the key factors of router resilience—withstanding attacks and effectively maintaining/returning service—are a personal responsibility that cannot be overstated, as individuals need to dispose of outdated routers and implement full security protocols protecting themselves as well as the US community as a whole. The choice remains in the owners’ hands to decide what level of security is implemented.

Only Private Owners Decide Smarthome Security-Privacy Tradeoffs—But Awareness Is Critical

The smarthome of science fiction is becoming a standard in today’s marketplace. The technology of the future is creating challenges which consumers have to reconcile concerning security, privacy, and convenience. Individuals embracing these conveniences in technology, which allow them to have everything from a talking refrigerator to an HVAC system that responds to their individual habits\(^ {27}\) and provide major conveniences in their lives, also open themselves up to security risks. Customers’ demands for technological advances in smarthome components
are outpacing predicted expectations. This could reveal consumers’ lack of concern for security, because these demands for new and innovative products are driving manufacturers to release devices before security is built in, exposing all consumers to risk. Knowing cyber criminals will take advantage of this vulnerability, it is left up to the consumer to assess personal value and convenience of smarthome components versus the risk of being hacked.

The significance of risk versus convenience of smarthome devices being linked to a financial institution is often not considered by many individuals. As stated earlier, a DDoS attack can originate through an individual’s smarthome devices accessing their financial institution. In an interview with Carter Holmes, manager of Goldenwest Federal Credit Union, a major concern was exposed with those individuals who believe that their limited account funds minimize their risk of being targeted for hacking. If a DDoS occurs, shutting down the information technology of their financial institution, and they have any type of Electronic Funds Transfers (EFT), serious unconsidered events could occur. While most consumers are used to the bank covering fraudulent credit card transactions, there are no such provisions if a financial institutions’ electronic payments are stopped. So if an individual’s insurance, mortgage, or utility payments are linked to their account via an EFT, financial institutions are not obligated to cover payments that are late. If action is taken by their mortgage, insurance, or utility companies, such as reconnection fees, late fees, or cancellation fees due to a DDoS attack, even those who feel they are not at risk of hacking due to limited personal funds can be sharply affected.

Armis, an IoT security solution provider, discovered threats they labeled “BlueBorne” security that offered sobering and revealing ways that hackers exploit IoT devices. They stated that nearly all Bluetooth devices could be exploited by attackers to spread malware and gain access to critical data and networks without user interaction. Icon Labs states that owners are not aware that current IoT devices can provide service for 15-20 years, much longer than a typical PC. Building devices that can evolve to ever changing security requirements by being updatable is not financially feasible; this creates future vulnerabilities for attacks, resulting in the abandonment of devices as the only security option. By 2020 Gartner Research predicts the IoT will be made up of 26 billion “units.” If manufacturers do not build and enable devices to adapt to the security needs, risks will grow exponentially over time.

The attitude of most consumers is that until there has been a high profile attack, they will take a “wait and see” attitude. It is challenging for consumers to gather data related to potential impact, regarding the exploits of cyberattacks, as it requires time and study to be obtained and without this information the decision process regarding security is faulty at best. The question is, with the data available, and the understanding that individuals have ownership and responsibility to determine their own levels of security and risk, due to the interconnected nature of the IoT, is this risk too high to be left to the individual? Again, “public buy in” to the need for security is essential for the support of secure devices and the maintenance of devices after market. If consumers do not accept the need for security protocols and implementation of best practices, the result may be a catastrophic event, which could drive the implementation of these security protocols by regulatory enforcement. Serious consideration should be applied by all individuals in their technology choices, as a service that brings us strength as a nation could also be used as a weakness to exploit. For overall safety, risk analysis should be carefully implemented during deployment and should continue as long as a threat is possible. One potential threat that still
needs to be analyzed for its impact to the consumer is the use of artificial intelligence (AI) and machine learning (ML).

**Cyber Attackers’ Ability to Control Smarthome Components Using AI Technology Imminent**

Within the field of artificial intelligence, machine learning is a branch of statistics and computer science that pursues the objective of programming machines to not only carry out specific cognitive tasks, but learn from the data they compile. While positive applications of artificial intelligence and machine learning are fueling part of the development of increasingly “smart” devices, the use of some tools within the broad AI domain for malicious intent is rising, and if trends continue, future years will surpass 2018 as the worst year for AI-powered cyberattacks as malicious actors find new vulnerabilities and use strategic attacks that are harder to defend against.\(^3\)

Artificial intelligence-powered cyber tools are not only being exploited to attack business resources, but to attack personal smarthome components as well. Estimates show that by 2021 spending on a wide range of artificial intelligence systems could reach $57.6 billion.\(^3\) With future expansion in the capabilities of AI systems, attackers will inevitably use the ability of AI-driven cyberattacks to blend in and go unnoticed while hitting vulnerable nodes to their advantage. A significant number of Americans regularly use devices with AI capabilities, but few recognize that AI technology is a part of their daily lives.\(^3\) Current smarthome components take advantage of AI functions to serve customers and collect data, but cyber attackers can use similar AI tools for exploitation of personal data.\(^3\) With over 127 million households in the US,\(^3\) and an estimated 15 devices per household,\(^4\) this would equate to billions of potential devices all susceptible to AI-driven cyber-attacks, and a treasure trove of data attractive to cyber criminals or foreign malicious exploitation. We are likely only beginning to see the threats and techniques which the abuse of AI could produce.

One of these techniques, phishing attacks, is not a new cyber threat. AI-controlled phishing attacks have a 30% greater success rate over traditional automated attacks, as the AI algorithms used have been trained to copy legitimate messages to execute attacks only a trained eye can detect.\(^4\) AI attacks on smarthome devices are rich treasures to cyber criminals, as over 70% of smarthome devices have security vulnerability related to weak passwords and inefficient default credentials as well as lack of data encryption, making smarthome components fully susceptible to AI brute force attacks.\(^4\) Brute force attacks are considered infallible, although they are a time-consuming approach.\(^4\) These attacks use automated tools to guess a combination of all legal passwords; the longer the password, the longer it takes to crack. The use of artificial intelligence enhanced with machine learning allows these brute force attacks to be more successful, as algorithms can be programmed to try commonly used passwords as well as utilizing a dictionary attack which tests for all words found in a dictionary to speed the process. Another security risk involving AI is that some AI-powered cyber tools now have the ability to infect networks without direct access to components from up to 229 feet away.\(^4\) This is a threat to nearly all US urban areas; older US urban housing setbacks are often directly on the street while modern urban housing setbacks are a minimum of 25 feet from the street,\(^4\) leaving the majority of smarthome components within US households susceptible to being accessed and
compromised by an AI-enabled device by a simple “drive by.” These cyberattacks would have no visual cues until an anomaly was discovered by the owner.

In general, actors with malicious intent will not attack IoT devices where security is in full implementation; they will use AI-powered “sniffers” to search for vulnerabilities in a network with little to no security to infiltrate the greater system. Sniffing is the process of monitoring and capturing all data packets passing through a network. By using sniffing, a cyber attacker monitors all data looking for very specific targets. When those targets are found, such as a password or account information, the algorithm is activated to take control. The principal advantage of this tactic is that once the system is infiltrated, the attacker basically waits patiently sorting through data until the vulnerability is exposed. AI-enabled tools excel at this style of attack, as it will seek out and continually search for vulnerabilities in the system even to the point where it will repeatedly visit the same sites to see if security is still maintained. This new genre of AI-driven programs have been trained to remain dormant until they reach a specific target within a network, which makes them extremely hard to detect and stop. No one has been caught utilizing this specific tactic for malicious intent, but in practice, several businesses and nation-state hackers have shown that the concept works. With this in mind the government should implement resilience best practices and security protocols for the manufacturers of smarthome devices and incentivize research of AI technology focusing on threat detection and protection to withstand cyberattacks of the future.

It can be argued that AI technology will soon become a part of everyone’s lives. Malicious attacks will continue to rise as adversaries and opportunists continue to attack unprotected resources. Known cyber attackers in 2018—responsible for brute force attacks and infecting systems with malware—included Chinese and Russian state actors, hacktivists, and others that investigators could not trace. Consumers need to realize that something as simple as a trusted smart light bulb, if not securely protected, could be the access point to breach their personal data, compromising their lives and potentially creating a greater security risk to the general public as a malicious cyber exploit spreads exponentially throughout the network.

**Smarthome Component Resilience Critical to Individuals, Business, and the Nation**

Smarthome devices achieve information technology resilience by developing the ability of a computer-based information system to withstand attacks with minimal to no security, financial, data, or proprietary loss. While individuals may find that some of their personal data such as grocery lists have no need for security, sensitive information and components can benefit from redundancy and resilience implementation. When there is a disruption of service, resilience determines the velocity at which that service can be restored. As US society becomes more reliant on computer networks and the interconnectedness the internet has brought in particular, the sustainability of the system becomes more critical to individual lives. In this context, resilience regarding the network affects individuals personally, as well as businesses, and even the government at the highest level.

Humans are responsible for the development of both the software and hardware needed to be resilient. When it comes to the storage of data, “the cloud,” a storage and service platform accessed through the internet, has totally changed information technology’s concept of
resilience.\textsuperscript{50} Anyone from individuals to small businesses and even the largest information technology companies can outsource the security and storage of their data on “the cloud,” which eliminates the high costs of maintaining their own storage facility; costs which can be prohibitive depending on the size of their needs. Major players can literally save millions of dollars in electricity bills by outsourcing to cloud services. These cloud service providers have a redundancy of stored data in multiple locations, so even if one facility is compromised, the backup facilities can upload the data to the customer with relative speed. Currently, major US cloud providers are Amazon, Azure, and Microsoft.\textsuperscript{51} Amazon Web Services (AWS) guarantees their service to 99.99999999999% satisfaction against loss of data, which arguably is as close to no risk as has been imagined at this time.\textsuperscript{52} Most cloud providers have different levels of security available. The private cloud is generally acceptable for most personal and business use, but the government cloud has even stronger security.

In discussing the resilience benefit of cloud services with Caleb Wilkinson, a lead Data Scientist for the Invista branch of Koch Industries, he stated that they contract out their service to AWS. He said the main question you need to ask yourself is, “Can you protect your data better than someone else?” In the last two years, Invista’s system only had a no-access problem one time. In the same time period they have had no loss of data, and their information is stored simultaneously at four locations, so even if one of the four locations were compromised, they would still have three other secure ones. If a site were to go down, AWS can have everything reloaded within 24 hours. One advantage of this arrangement for individuals and companies is that the subcontractor (the cloud service provider) has the worry of security/resilience. Another advantage is that in the case of Invista, AWS does all the patches and updates, so as technology and the threat of cyberattacks evolves, the organizations with most responsibility over critical data are focused on the specific skill set of protecting assets so private entities do not have to be. Concerning whether cloud services are the right route for individuals or an entity to pursue, Wilkinson said: “One needs to determine the cost of the private server necessary compared to the worth of their assets, to see if an outside service would fit their needs.”\textsuperscript{53} The advantage of cloud services to consumers is that the same high level security available for the business world is available to them as well. With implementation and use of the cloud across all platforms, security is enhanced for the network as a whole, which is a big benefit to the consumer as well as the public sector.

Cloud services can also alleviate risk to the individual when hardware fails. As stated previously, if network services are compromised, with financial and medical data being the most at risk, the redundancy provided for the consumer at a personal level also at a larger network level is reassuring. When it comes to the hardware in the information technology field, keeping a replacement supply of units available and ready to use is a common practice. Companies recognize the high value loss potential when even a minute without hardware or software services can cost the company. It has been estimated that when a data center goes down across industries, the cost is roughly $5,600 per minute.\textsuperscript{54} Cloud services can also be an advantage to the private consumer in financial savings as impact is minimized to those who would rarely have extra hardware on hand. Thus if individuals smart home devices are compromised, they can be assured that their data will be maintained. Cloud providers can tailor the security and access to their services to specific requirements to the benefit of consumers.
Hardware longevity, according to Dr. David Olsen, head of the Management Information Systems (MIS) department at Utah State University, has as a general rule that any device two years or older needing service is thrown away because of the rapid pace of technology advancing and the costs of service exceeding that of replacement. He also stated that it was critical to know both your system’s scope and value and that: “The best thing to do is to test as hard as possible to start with; the tougher the testing processes the more reliability and resilience you will have in the future.” In the industry, the “Mark of Excellence” is determined by the toughness of the initial testing. Consumers should implement the same high standard of testing in deploying their own smarthome devices.

Best resilience platforms coupled with security protocols will minimize individuals’ risk in the short and long term. One of the greatest advantages of taking the mindset of resilience is proactively facing the reality that a security or system failure may occur; because with failure the greatest opportunity for innovation occurs for building future resilient characteristics into products and solutions to protect the network as a whole.

Conclusion: Smarthome Devices Will Work For Us Or Against Us

Individuals love their lives to be more convenient. Smarthome components with their ability to react to individual tastes and needs have a bright future for innovation. But with these conveniences, there is often another side of the coin that can be exploited by those who have malicious intent. Criminals and foreign adversaries have not been inhibited in the past from carrying out malicious attacks, and there is little chance of the cyber enemies of the future, in all their various forms, being any different. Government and manufacturers of smarthome devices still have an inherent responsibility to look after society as a whole due to the interconnected nature of the current system of networks, seeking where possible to shore up the security of the network as a whole despite the reality that some individuals will be dismissive with regards to their own security. But at the end of the day, individuals are responsible to be their own first line of defense and to do their part to secure their world around them, which applies to their smarthome components and the interrelationship with the IoT. While future cyberattacks are inevitable, the more that is done to protect the network and individual devices now will help facilitate the “rebuilding” that occurs after such attacks, allowing more resilience not only for the individuals but businesses and government as well. The reality is—if you are going to use smarthome devices, establish security protocols or “don’t risk more than you can afford to lose.”
Endnotes

7 Abigail Summerville, 2017, CNBC “Protect Against the Fastest-Growing Crime: Cyber Attacks.”
9 Scott Robinson, 2019, “Smart Home Attacks Are a Reality, Even as the Smart Home Market Soars.”
10 TechTarget SearchSecurity 2017, “How to Prepare for the Emerging Threats to your Systems and Data.”
https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
11 Dr. Eric Hawley, CIO of Utah State University, Logan, Utah; interviewed 3/29/2019.
12 NORTON Authored by a Symantec employee, 2019, “12 Tips to Help Secure Your Smart Home and IoT Devices.”
14 Dr. Jacob Gunther, Department Head of Electrical and Computer Engineering at Utah State University, Logan, Utah; interviewed 3/28/2019.
15 Dr. Eric Hawley, CIO for Utah State University Logan, Utah; interviewed 3/29/2019.
https://www.dhs.gov/topic/cybersecurity
19 NORTON Authored by a Symantec employee, 2019, “Targeted Attacks Now Moving Into the IoT & Router Space.”
21 Tomas Foltyn, 2018, “Most Routers Full of Firmware Flaws that Leave Users at Risk.”
https://www.pentasecurity.com/blog/4-shocking-iot-security-breaches-2018/
23 Christian Foss, 2017, “Social Engineering is the Greatest Threat Against Secure IoT.”
https://info.addsecure.com/social-engineering-is-the-greatest-threat-against-secure-iot
24 Executive Office of the President, 2018, “The Cost of Malicious Cyber Activity to the U.S. Economy.”
www.us-cert.gov/china
https://www.pentasecurity.com/blog/4-shocking-iot-security-breaches-2018/
30 Ashwin Pal, 2019, “The Internet of Things (IoT) – Threats and Countermeasures.”
31 Carter Holmes, Manager for Goldenwest Federal Credit Union, Logan, Utah; interviewed 4/24/2019.
32 Michael Dortch, 2018, “The Internet of Things (IoT): What You Need to know and Do Now.”
https://www.itchronicles.com/iot/internet-things-iot-need-know-now/
33 Alan Grau, 2018, “Internet of Secure Things.”
34 Ashwin Pal, 2019, “The Internet of Things (IoT) – Threats and Countermeasures.”
35 Deepak Dutt, 2018, “The Year of the AI-powered Cyberattacks.”
36 Bluefin, 2019, “AI and the Cyber Attacks of the Future.”
https://techcrunchies.com/tag/iot/
38 Deepak Dutt, 2018, “The Year of the AI-powered Cyberattacks.”
https://blog.avira.com/the-true-cost-isps-pay-for-weak-iot-security/
https://blog.avira.com/the-true-cost-isps-pay-for-weak-iot-security/
43 Margaret Rouse, 2019, “What Strategy Do You Use to Protect Against Brute Force Attacks?”
https://searchsecurity.techtarget.com/definition/brute-force-cracking
44 John Markoff, 2016, “Why Light Bulbs May Be the Next Hacker Target.”
https://codes.iccsafe.org/content/I2C2018/chapter-5-residential-zones
46 Jignasa Sinha, 2018, “5 Artificial Intelligence-Based Attacks That Shocked The World In 2018.”
47 Joseph Menn, 2018, “New Genre of Artificial Intelligence Programs Take Computer Hacking to Another Level.”

https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types

https://wiki.ittc.ku.edu/resilinets/Main_Page

https://searchcio.techtarget.com/definition/business-resilience

https://www.datamation.com/cloud-computing/cloud-computing-companies.html


https://deloitte.wsj.com/cio/2013/04/01/how-to-create-it-resilience/

55 Dr. David Olsen, Department Head of Management Information Systems in the Huntsman School of Business at Utah State University, Logan, Utah; interviewed 3/29/2019.