Cybersecurity in the Age of Connected "Things"

By Pete Slade
ICIT Fellow and Founder and Chief Scientist, ThreatWarrior

There is no denying it: smart technology has penetrated almost every aspect of modern existence. From virtual assistants and self-driving cars to security cameras and smart vending machines, our homes and offices are filled with more internet-connected devices than ever. However, there is an often-overlooked risk involved with widely and rapidly adopting these technologies: the additional attack vectors they open to cybercriminals.

The Internet of Things and Threats

Cyberattacks involving Internet of Things (IoT) devices are surging at an unprecedented rate. Our hyper-connectivity and reliance on IoT devices provide myriad conveniences, but they also create cybersecurity blind spots across consumer markets and enterprises.

IoT devices are often not designed with security in mind. They are versatile, yet vulnerable. Built with limited security controls, these devices are commonly targeted by cybercriminals and used to launch attacks on other parts of the networks connected to them. A single threat to any part of the system can compromise the entire network. For example, in 2016, the Mirai botnet launched the largest ever distributed denial of service (DDoS) attack using an IoT botnet. It exploited vulnerabilities in IoT devices such as DVRs and digital cameras. Once infected with Mirai, computers would continually search the internet for vulnerable IoT devices, then infect them with malware.

> *"IoT devices are often not designed with security in mind. They are versatile, yet vulnerable. Built with limited security controls, these devices are commonly targeted by cybercriminals and used to launch attacks on other parts of the networks connected to them."*
>
> \- Pete Slade
> Founder and Chief Scientist
> ThreatWarrior

The victim of the attack was Dyn, a company that controls much of the internet's DNS infrastructure, bringing down high-profile sites as CNN, Twitter, and Netflix for the majority of an entire day. Dyn estimated that "100,000 malicious endpoints" were involved in the attack. The Mirai botnet was able to achieve this scale because it hacked so many internet-connected devices. In the end, it was determined this attack was carried out by a non-state actor, but the implications are frightening. Imagine what a state-sponsored actor with disposable resources could do with insecure IoT devices!

In 2018, the US actually had a brush with this when a Russian APT hacked into residential routers and had them looking for Ukrainian NAS drives to infect. The attack was caught and ultimately stopped by Cisco Talos and the FBI. They issued a statement directing everyone to remediate by resetting their routers to disrupt the malware, identify infected devices, and download updates. The crisis was averted, but attacks like this have the potential to cause massive damage.

Why are IoT devices such a threat?

While IoT devices are not necessarily new, they are still in their relative infancy, and some industries are only just beginning to use them. That has not stop internet-connected devices from flying off the shelves. They are quickly adopted for the conveniences they offer, even if users do not fully understand the risks involved.

As mentioned above, IoT devices are typically built with 'convenience-first design principles,' not security-by-design principles. This makes them easy targets for hackers who can use them as stepping stones into other parts of the network, and why threats to IoT ecosystems can quickly evolve into greater security risks.

Internet-connected devices gather a lot of data from their users and environments because it is necessary for them to function and deliver efficiencies. However, if these devices are compromised, it could lead to many other consequences, including full-network breaches, theft of all that data, and shutting down entire businesses.

IoT Attack Vectors

The Open Web Application Security Project has published a draft of IoT attack vectors as part of its Internet of Things Project. The list details areas in IoT systems that may present cybersecurity vulnerabilities. The list should be understood by device manufacturers, security experts, IT teams, and anyone planning on deploying connected technology in their organizations. Attack vectors include:

- **Devices** - The most widely recognized attack vector in IoT environments are devices. This includes anything connected to the internet, from cell phones, laptops, and servers, to less typical devices, such as video cameras, industrial control systems, smart printers, and thermostats. Attackers can exploit device firmware, ports, web interfaces and exposed APIs, while also taking advantage of weak passwords, unencrypted data, outdated components, and weak privilege escalation.
- **Applications** - Web applications and IoT device software can also be used by hackers to compromise entire networks. Insecure data storage, weak passwords, deficient access controls, or ineffective authentication can easily lead to breaches. Additionally, the hyperbolic growth of microservices combined with the heightened complexity of microservice architecture expands the attack surface, making application security an even bigger factor. As we move into the future, monitoring applications and threats at scale will require even more automation.
- **Communication Protocols** - The channels devices can use to transmit data or send and receive commands can also be targeted by hackers. Unsecured public-facing Wi-Fi, misconfigured protocols, update pushes, and network attacks like DDoS can affect these critical channels.

You may remember the Amazon Ring attack from Dec. 2019, in which hackers were able to access Ring's smart security devices. Unbeknownst to the owners, hackers used Ring to watch and even communicate with people. In a disturbing breach of personal privacy, one incident in Mississippi allegedly involved a hacker communicating with an 8-year-old girl via the Ring camera in her bedroom. In Alabama, a hacker allegedly spoke to children playing basketball outside their home, encouraging them to move closer to the camera.

This is a perfect example of bad actors taking advantage of vulnerabilities in IoT devices. Ring's web accounts did not require owners to utilize two-factor authentication, which enabled hackers to log into them with information found through an online database of previously compromised information.

Similarly, this is another reminder that convenience often comes at the cost of security. Ring could require multi-factor authentication; biometric security, such as face scanners or fingerprint readers; or a process by which device owners must confirm any new attempted sign-ins. However, because (like many IoT device manufacturers) Amazon wanted to remain easy and convenient for the end-user, they choose not to implement stricter security measures.

Security Needs to Start with the Manufacturers

Beyond organizations updating their own cybersecurity strategies to consider emerging technologies, the increasing number of IoT hacks highlights the crucial responsibilities of IoT device manufacturers.

Product liability law assigns responsibility for defective products to the device manufacturer. If a product malfunctions and causes personal harm or property damage, the manufacturer is liable for that claim. The user does not need to prove negligence. These traditional laws translate reasonably well to situations where the hardware of an IoT device malfunctions. However, because IoT devices are a mix of hardware and software, proving liability becomes a more complex process.

Liability for security breaches and invasions of privacy do not fit into traditional liability laws. Because there is not yet a defined, universal standard for IoT security, if there is a malfunction that does not cause physical damage (for example, a breach of privacy opposed to bodily injury), it is difficult to prove specific harm to the user. In the past, courts have typically ruled that software is a service, not a product. This means that software manufacturers are not held to a specific set of standards like hardware manufacturers. However, IoT devices are a mix of these components, and both need to function properly for the device to work. It is clear there needs to be an evolution of product liability laws to accommodate the rapid growth and adoption of connected things.

In truth, it is easier and cheaper for manufacturers to sell internet-connected devices with low-quality security controls. Maximum convenience and an inexpensive price often come at the expense of loosened security policies. IoT device manufacturers need to carefully consider security-by-design principles, creating connected devices with security in mind from the ground up. Without benchmarks and best-practice standards for the security of connected “things”, these low-hygiene devices will continue to flood the market.

> *“It is critical that we address cyber threats at a federal level. As cyber threats continue to evolve, we too must change the way we think about and tackle them.”*
>
> *- Pete Slade*
> *Founder and Chief Scientist*
> *ThreatWarrior*

It is critical that we address cyber threats at a federal level. As cyber threats continue to evolve, we too must change the way we think about and tackle them. We need to prioritize creating strict security standards around IoT devices. Programs like the Cyber Shield Act, which would encourage and incentivize manufacturers to adopt best cybersecurity practices when developing these products, is a good place to start. The Cyberspace Solarium Commission is a congressional council designed to create a comprehensive cybersecurity strategy for the United States in a time when cyber threats are escalating at an unprecedented rate. By formulating new polices, the Commission seeks to drive the safety of critical infrastructures through changing legislation and other initiatives.

Not If, But When

> *"It is estimated there will be more than 75 billion connected devices in homes and businesses around the world by 2025. Without the proper security, each of them is an attack vector for corporate espionage, government data theft, or the planting of malware to wreak havoc on a critical infrastructure system."*
>
> *- Pete Slade*
> *Founder and Chief Scientist*
> *ThreatWarrior*

Who should be held reliable when an attack inevitably occurs? Liability is a continuum. While a security-by-design strategy may start with the manufacturer, they are not the only relevant players on the field. System integrators, cybersecurity experts, IT specialists, executives, and more need to employ wide-scale collaboration to create truly comprehensive security strategies.

Again, liability exists on a sliding scale. Who takes the blame for negligence when a breach occurs? Can the fault always be attributed to a single party? Responsibility needs to start with the manufacturer, but integrators who combine multiple connected products to provide solutions to their customers also share accountability, as do cybersecurity experts and IT specialists. Additionally, the end user needs to follow proper cyber hygiene and security best practices at all times. It is a shared responsibility at every step, though the legal system tends to lag behind the pace of technological evolution.

It is estimated there will be more than 75 billion connected devices in homes and businesses around the world by 2025. Without the proper security, each of them is an attack vector for corporate espionage, government data theft, or the planting of malware to wreak havoc on a critical infrastructure system.

We are all aware of the dangers lurking in cyberspace, but many organizations are still not vigilant enough in protecting themselves or their clients. Often, they take a "Well it hasn't happened yet… Who would want to hack my business?" stance.

However, it is no longer a question of if, but when. Nefarious cyber actors will attempt to breach your systems, and with IoT devices, rogue operatives have more avenues of attack than ever before. We all need to work hard to ensure they are not successfully breaching IoT devices.

Legacy Cybersecurity Cannot Protect the Modern Enterprise

With new internet-connected devices constantly being added to enterprise ecosystems, new attack vectors arise daily and threats constantly evolve to evade traditional security measures. In the age of IoT, first-generation cybersecurity tools like agent-based solutions, log readers, and cloud-only security are not enough to defend against modern cyberattacks.

Agent-based solutions are not necessarily *bad* solutions. They are actually helpful in delivering device-level analytics and context. However, agent-based solutions are only partially effective. They only protect machines they are installed on and are typically blind to everything else. While there are, of course, agents for desktops and servers, many smart devices like printers, smart vending machines, and security cameras lack the interfaces to support these software agents, even if they were available. These connected devices were not designed with security in mind and were not meant to accommodate third-party software installation. As more of these connected 'things' are added to networks, often without approval or oversight, it is critical that security teams implement technologies that can discover and defend them.

The exploitation of insufficient logging and monitoring is the root cause of most breaches. Hackers rely on this to hide in networks. The problem with log readers is that they only track existing logs, and logs can be modified as evidenced in the recently-released indictment against the People's Liberation Army, the armed forces of the People's Republic of China, who breached Equifax in 2017. The indictment alleges that, in order to conceal their identity, the hackers configured settings that "wiped log files on a daily basis in an effort to eliminate records of their activity." Clearly, if an attacker changes or wipes the log data, it becomes impossible to track a threat moving through the network.

> *"The more connected we become, the more critical it becomes that we maintain our focus on cybersecurity and innovating to keep pace with the growing number of "things" we are connecting to our networks."*
>
> *- Pete Slade*
> *Founder and Chief Scientist*
> *ThreatWarrior*

Additionally, the increasing use of microservices only exacerbates the weaknesses of log-reading systems. Microservices are distributed and stateless, leading to more logs to monitor, which results in an overload of logs, potentially concealing security issues. User logging needs to correlate context and events across different, decentralized platforms in order to be effective. At scale, automation will be required to monitor these logs.

Lastly, cloud-only security systems leave massive holes in an overall defense strategy. Cloud security is necessary, but businesses do not fully operate within the cloud. Enterprises have offices and firewalls, and people working behind them. Cloud-only solutions cannot protect against on-premises incidents, requiring a hybrid approach.

Especially now in the midst of a global pandemic, we've seen just how far cybercriminals will go to take advantage of every vulnerability in traditional security solutions. During COVID-19, medical ecosystems – some of our most critical network infrastructure -- have experienced a barrage of cyberattacks as malicious actors continue to exploit exhausted IT teams and medical devices built without security-by-design principles.

That's why ThreatWarrior takes a network-centric approach to cybersecurity using unsupervised neural networks. Our advanced technique allows organizations to stop emerging threats by helping them see the signal through the noise, learn the behavior of every user and device connected to the network, and immediately act on that information.

For example, consider a large-scale phishing attack against a healthcare organization. All it takes is one employee to inadvertently allow cybercriminals access to the entire network. Health organizations rely on wired and wireless networks to connect mission-critical resources, so a single point of compromise could be catastrophic.

Consider if one unsuspecting employee allows malware into the medical ecosystem, which then moves laterally through the network, infecting unprotected devices, bringing down smart beds, monitors and EMRs, or even encrypting a computer in the operating room. In healthcare organizations, these breaches could cost human life.

ThreatWarrior would identity this abnormal behavior caused by the malware, autonomously quarantining devices to prevent the spread and alerting a security team to take further action. Many legacy security solutions may not even be able to see the devices that are being infected and therefore cannot stop it, which is what makes using advanced cybersecurity so vital to conducting business in the age of connected things.

Securing the IoT

As we all know, our data is used and shared between more platforms than ever. The more connected we become, the more critical it becomes that we maintain our focus on cybersecurity and innovating to keep pace with the growing number of "things" we are connecting to our networks. To create a truly comprehensive cybersecurity strategy, organizations have to consider every IoT device as an avenue of compromise. It really is a zero-trust world.

Outside of updating and rethinking security strategies, there are many steps which will help protect your business or home from breaches. They are commonly known to many, but it is never a wasted exercise to reevaluate and double-check cyber policies. These include:

- **Education** - Consumers need to be educated on how to protect their own privacy and personal data while enterprises need to ensure data security to protect their economic well-being, client data, and brand reputation. There are many educational resources available, and you should always research built-in security mechanisms before buying and implementing IoT devices into your ecosystem. Ensure they utilize strong password protection and user authentication, encrypted communication, and hardened physical components.
- **Proper Cyber Hygiene** - This is a basic, but critical, factor in keeping your network safe from cyberattacks. Always use unique passwords and strong multi-factor authentication whenever possible, install antivirus and malware software, employ device encryption, and regularly perform updates and back up data.
- **Updated Technology** - In many businesses, IoT devices are added without oversight from security or IT teams. Bring Your Own Device (BYOD) policies pose an additional danger here. It's critical that your security controls can properly see and manage all assets connected to your network. First-generation security solutions are no longer effective in today's constantly-evolving threat landscape.
- **Zero-Trust Architecture** - Organizations should not trust by default. Do not assume that anything inside or outside your network is safe. In fact, do the opposite. The line between "inside" and "outside" a modern business network has become so blurred, you must operate on the assumption your business could be compromised by anything.
- **Physical Security** - If an IoT device lacks any physical safeguards, cybercriminals could tamper with or exploit them. You may not be able to restrict access to every IoT device on your network but using locks or other tools, where possible, will provide an additional layer of security against bad actors.

The proliferation of IoT devices has undoubtedly changed the business landscape and with it, the threat landscape. Increasing security incidents involving connected devices emphasizes the need to consider evolving technologies when developing security strategies.

Securing the IoT is a challenging task that requires large-scale collaboration and effort, but it must be done. Cybersecurity can no longer be an afterthought. You must harden your defenses with the mindset that the wellbeing of your organization is at stake. Because it is.

About the Author

Pete Slade is the Founder and Chief Scientist of ThreatWarrior. Pete Slade is the visionary behind ThreatWarrior's groundbreaking cyber defense platform. He is an expert in threat intelligence and network security, with proven success building advanced threat intelligence, detection and response solutions. Pete has more than 30 years of experience in cybersecurity, information technology, and machine learning, having designed and built systems for both commercial and intelligence communities. He is a regular public speaker on the topics of cybersecurity, national defense, AI, and entrepreneurship. Pete is also a patented inventor, a Fellow at the Institute for Critical Infrastructure Technology, a member of Forbes Technology Council, and a congressional advisor on the topics of systems and infrastructure security.

Pete leads the company's threat intelligence team and drives research and development of ThreatWarrior™, the industry's most advanced threat intelligence platform. ThreatWarrior leverages a state-of-the-art behavioral platform to learn the behavior of every human and device on the network, combined with real-time network traffic analysis, threat intelligence, incident forensics and automated response to keep organizations ahead of constantly-evolving cyberattacks.

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.