CyberReady™

Cyber Security Assessment
For Homes and Real Estate
https://cyberreadyassessments.com/

The Opportunity for SmartHomes

As buildings become smarter, the risks associated with the theft of data grows. Residential Real Estate needs a way to assess and evaluate the cyber risks of homes. Much like environmental or health scoring models, CyberReady™ provides a comprehensive assessment of the property and a score that can be used as a benchmark moving forward. It can also serve as a valid assessment for cyber insurance, a road-map guiding what to fix and spend and suggest mitigation safety measures about the IoT and connected items around a home.

The Problem

In a competition to gain more convenience, personalized and comfortable services, homes strive to enhance automation and technology interface. All of this comes at the cost of cyber risks. Following marketing appeal and social trends, homeowners must also address and protect their data privacy.

The most dangerous security threats for homes include:

- ✓ Physical: homes are becoming smarter with interconnected smart meters, thermostats and doorbells, just to name a few. Many of these devices provide third parties access to this interconnected infrastructure.
- ✓ Behavioral: lack of awareness or training regarding IoT devices around the home, telecommuting safe procedures; phishing attacks; too casual uses of social media
- ✓ Technical: between wifi routers, printers, personal and work devices, gaming consoles and home automation, the average home has a complex communication and processing ecosystem that often transfers personal and sensitive data.

Cybercrime is increasing and changing.

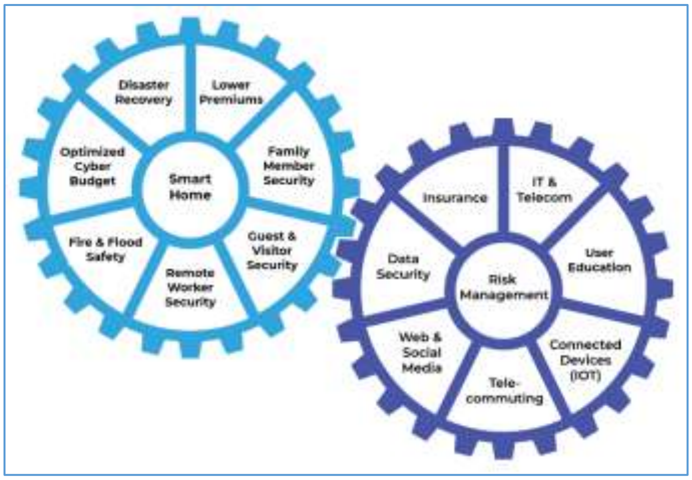
The expanding threat landscape and new business innovation is leading to an increase in cyberattacks – the top 5 data breaches of 2019 had a combined breach of over 3 billion records. https://www.safety.com/biggest-data-breaches-2019/

Evolving targets: Information theft is the most expensive and fastest rising consequence of cybercrime. But data is not the only target. Core systems, such as smart meters and Internet of Things (IoT), are being hacked in a dangerous trend to disrupt and destroy. Attacks on IoT devices tripled in the first half of 2019 (CSO online).

Evolving impact: While data remains a target, theft is not always the outcome. A new wave of cyberattacks sees data no longer simply being copied but being destroyed. Attacking data integrity—or preventing data toxicity—is the next frontier.

Evolving techniques: Cyber criminals are adapting their attack methods. They are targeting the human layer—the weakest link in cyber defense—through increased ransomware, phishing and social engineering attacks as a path to entry.

SmartHome Risk Management Ecosystem



The Solution

A holistic risk assessment, based on leading security frameworks (GDPR, ISO, NIST, FIPS, FISMA), that allows households to quickly and easily assess the risk exposure of their homes systems and how they use them across three critical areas – Physical, Behavioral, and Technical. From those findings, a report outlining a path forward for corrections is generated, providing a pathway for continuous monitoring and improvement of your smart home. Site visits are available should you need help updating your equipment settings.

SmartHome™ is a simple-to-use, yet robust assessment across 12 attributes that summarizes the findings across the three areas and provides an overall score for the home and implementation guidance to improve it.

In addition to SmartHome, our suite of assessments includes:

SmartOffice™	https://cyberreadyassessments.com/smartoffice
SmartTenant™	https://cyberreadyassessments.com/smarttenant
SmartHotel™	https://cyberreadyassessments.com/smarthotel
SmartInsure™	https://cyberreadyassessments.com/smartinsure
SmartRemote™	https://cyberreadyassessments.com/smartremote

The Team

Michael Savoie, PhD has been involved in cybersecurity for over 25 years. He has worked on cybersecurity programs for the US Departments of Energy and Defense, and National Security Agency. He developed the algorithms on which CyberReady™ is based in 2012.

Noëlle Brisson FRICS, MAI, has an international career in commercial real estate and operational reviews, focusing on valuation and underwriting and portfolio asset management where data quality, reliability, protection and governance are essential.