



IoT

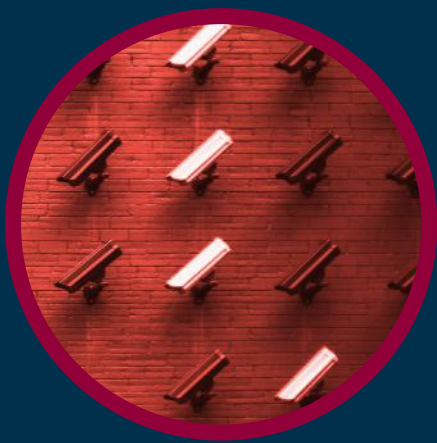
— And

Physical Security

kISI

Whitepaper Series

Overview



- 5** **Tech Startups, IoT,**
And The Need For New Security Systems
- 7** **Fear of IoT-Enabled Security**
Among IT Departments
- 9** **The Cost of Security Breaches**
Global, Multi-Industry Threats
- 10** **The Need For**
IoT-Enabled Physical Security
- 12** **Physical Security**
Marketplace by System
- 13** **How Should**
The Physical Security Market Approach IoT
- 16** **Why**
IT Departments Need To Own
Physical Security
- 17** **Cyber Security Firms**
And IoT-Enabled Physical Security
- 18** **Bringing Physical Security**
Into The 21st Century

“While the rise of IoT creates more entry points into data systems through the connectivity of physical objects, IoT can also enable data protection through the connectivity of a physical security system.”

In a world filled with cyber security threats and breaches from major corporations to governments to startups, physical security is often overlooked. Experts suggest that physical security is of vital importance to information security, as physical theft and insider threats are rampant. This paper examines the data security and business culture implications of IoT-enabled, physical security systems, such as cloud-based access control and smart keyless solutions, and how they allow tech startups to have more control over their physical security and data than traditional environmental locks. This paper also explores the idea that because physical access can be a cyber security threat to a company's data, facility control should be a function of IT departments.

Tech Startups, IoT,

And The Need For New Security Systems

According to the [GEM Global Report](#), there are over 100 million startups formed every year across the globe. Startups are not only an integral part of the technology sector's evolution and global economic growth, they are instrumental players in keeping the tech industry secure.

However, among the plethora of cash-strapped startups that prioritize product development, raising capital, and scaling fast—all while working with minimal resources first and foremost—data security is often ignored. This makes startups a prime target for cybercrime.

To understand security needs of tech startups, the rise of the Internet of Things (IoT) must be taken into consideration. Gartner estimates that currently [5.5 million new](#) things are being connected to the internet every day, and that this figure will reach 6.4 billion by the end of 2016.

For technology companies of all sizes, IoT is opening up opportunities for developing new products across industries that can be enhanced with networking capabilities. Additionally, IoT technologies are aiding startups in their ability to monitor and control information, as their application can lower maintenance costs by [25% and minimize outages by 50%](#).

Thus, the IoT trend is helping startups run their operations differently, while simultaneously shifting and expanding the business world's view on information technology. Additionally, the IoT market has broken new ground for startup innovation. Case in point: the international market for wearables has increased 223% this year, according to [IDC](#).




"...there are over 100 million startups formed every year across the globe."

-GEM Global Report



In the same vein, IoT is increasing concerns around security, as connecting the ubiquitous world of “things,” from devices to appliances to cars, creates new access points to potentially be hacked. In 2015, [HP reported](#) that up to 70% of commonly used IoT devices are vulnerable to cyber attacks and breaches.

70%  **” In 2015, HP reported that up to 70% of commonly used IoT devices are vulnerable to cyberattacks and breaches. ”**

According to a report by AT&T, titled [“The CEO’s Guide to Securing The Internet of Things,”](#) 90% of organizations lack full confidence in their IoT security. The bottom line is that while IoT can have a significant positive impact on a company’s operations, it can also put the company’s security at risk.

Now more than ever new security tactics and tools are needed, due to the proliferation of the IoT market, which is expected to grow from USD 157.05 billion in 2016 to USD 661.74 billion by 2021, according to the [“Internet of Things \(IoT\) Market - Global Forecast to 2021”](#) report by [Research and Markets](#).

In today’s IoT-enabled and data-driven landscape, ensuring a team can focus on creating the value its investors are looking for means investing in security awareness and proper security systems, both technologically and culturally, as security breaches put a IP at risk and take time away from innovating.

For this reason, the concept of [security by design](#)— incorporating core security features at the earliest stages of development—is paramount. The term was coined by Federal Trade Commission Chairwoman Edith Ramirez. This practice and investing in up-to-date tools is imperative.

However, some of the most trusted and disruptive technology companies don’t have the bandwidth or resources to embed security measures at such an early stage. While they are modern and tech-enabled, many startups have out-of-date-security systems.

Security expert Bill Ho, CEO of Biscom, says security breaches are not solely an IT problem. He opines that security is an organizational issue that has both technology and personnel factors to consider.

“While IT security can always be improved with newer detection and prevention systems, many companies would gain more value from improving the security culture and awareness of its employees,” said Biscom.



” Now more than ever new security tactics and tools are needed, due to the proliferation of the IoT market, which is expected to grow from USD 157.05 billion in 2016 to USD 661.74 billion by 2021, according to the “Internet of Things (IoT) Market - Global Forecast to 2021 ”

- report by Research and Markets.

One method for educating the employees of tech startups and large tech firms is showing them the impact of new security tools in the cloud and physical world, also know as IoT-enabled physical security, which utilizes the very trend that many IT departments view as a serious threat to security.

“ There have been instances of IoT devices constantly sending information back to their manufacturers—smart TVs recording what you are saying and surveillance cameras communicating with a large P2P network - *said Bell* ”

“ There has even been a case of a digital video recorder (DVR) device that’s sold in tandem with Internet-enabled surveillance cameras sending data to a third party or an embedded P2P network. ”

Fear of IoT-Enabled Security

Among IT Departments

Due to fear IoT among IT departments, there is fear to adopt IoT-enabled security systems. Steve Bell, Security Expert for BullGuard, says a number of IT divisions have concerns about businesses pushing IoT onto them without considering the security implications.

“There have been instances of IoT devices constantly sending information back to their manufacturers—smart TVs recording what you are saying and surveillance cameras communicating with a large P2P network,” said Bell. “There has even been a case of a digital video recorder (DVR) device that’s sold in tandem with Internet-enabled surveillance cameras sending data to a [third party or an embedded P2P network.](#)”

Bell explains that when this occurs it’s important to ensure IoT devices can get the best connection possible.

“You could imagine an IT manager having sleepless nights knowing that his or her company IoT devices are enabling P2P communications,” said Bell. “Added to this, IoT device default settings often ignore security and privacy concerns. This is assuming that IT departments have some awareness about the potential vulnerabilities. Many don’t. This is illustrated by the large number of IoT devices tagged by the Shodan search engine that have open ports. An open port is like an open door. It’s an invitation for the mischievous and those intent on carrying out some form or criminal endeavor.”

The biggest security breaches of 2015 include a number of high profile companies.



Source:

Slack • Hacking Team • Kaspersky • CareFirst Bluecross BlueShield
LastPass • Premera BlueCross BlueShield • Experian • T Mobile
Office of Personal Management • Ashley Madison

The Cost of Security Breaches

Global, Multi-Industry Threats

Depending on the type of breach, companies may lose revenue, competitive advantage, the health and safety of employees, or all of the above. In severe cases, a breach could lead to the financial downfall of a company.

Nortel Networks is a perfect example. Chinese hackers gained access to Nortel's network and downloaded business plans, research and development reports, employee emails and other documents. Security experts within the telecommunications giant blame the security breach for its bankruptcy.

PGP Corporation, a global leader in enterprise data protection, and the Ponemon Institute, a privacy and information management research firm, conducted a study in 2013 on the U.S. Cost of a Data Breach. According to the study, data-breach incidents cost U.S. companies \$204 for each compromised company in 2009, compared to \$202 in 2008. Despite an overall drop in the number of reported breaches (498 in 2009 vs. 657 in 2008, according to the Identity Theft Resource Center), the average total per-incident cost in 2009 was \$6.75 million, compared to an average per-incident cost of \$6.65 million in 2008.

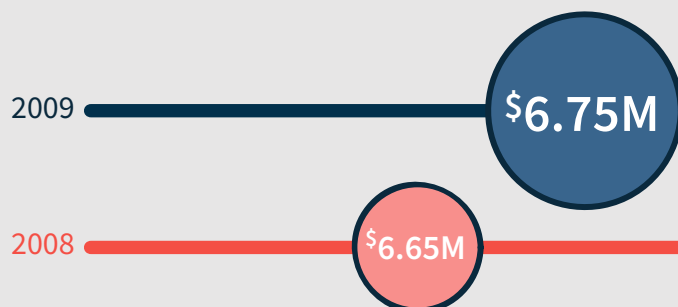
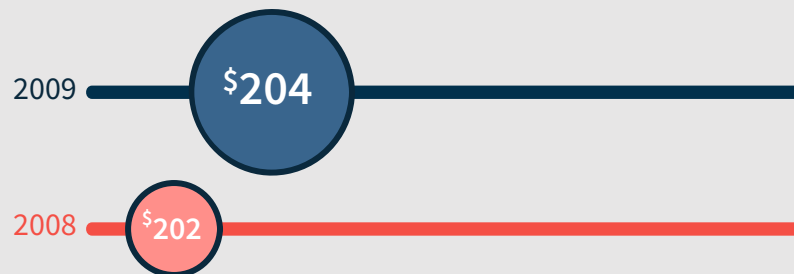
Another study conducted by the Ponemon Institute revealed that security threats are a global and multi-industry issue costing billions of dollars. The average annualized cost of cyber-crime for 56 organizations in the study was \$8.9 million, with a range of \$1.4 million to \$46 million in 2010. In 2011, the average annualized cost was \$8.4 million. This represents an increase in cost of 6% or \$500,000 from the previous year.

The companies in the study experienced 102 successful attacks per week and 1.8 successful attacks per company per week. This represents an increase of 42% from the previous year's experience.

According to [The 2013 Cost of Cyber Crime report](#), sponsored by HP Enterprise Security Products, the most costly cyber crimes are caused by "denial of service, insiders and web-based attacks."

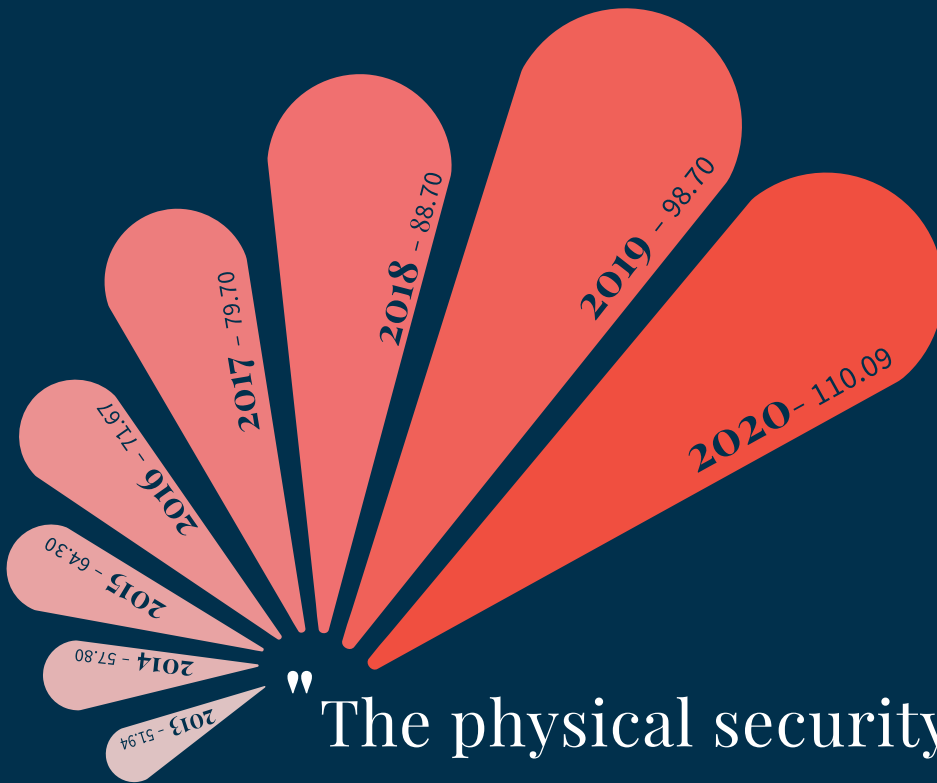
Data Breach Cost

According to the study, data-breach incidents cost U.S. companies \$204 for each compromised company in 2009, compared to \$202 in 2008.



Per-incident Cost

Despite an overall drop in the number of reported breaches, the average total per-incident cost in 2009 was \$6.75 million, compared to an average per-incident cost of \$6.65 million in 2008.



“The physical security market has been valued at USD 51.94 billion in 2013 & is likely to reach a value of USD 110.09 billion by 2020, growing at a CAGR of 11.3% from 2014 to 2020. The global physical security system market was valued at USD 51.94 billion in 2013.”

– *GrandViewResearch.com*

The Need for

IoT-Enabled Physical Security

The question is, can the trend and tools that caused this vulnerability be re-appropriated to make a company's data safer? A number of physical security experts and IoT-enabled security providers and users believe they can.

"The internet of Things (IoT) continues to forge new integrations between a vast, ever-growing array of systems, sensors, devices and services. With unbridled connectivity of sensors to people, processes and things, once disparate systems, such as physical security, will be a critical part of the IoT."
-Security Journalist, Debora O'Mara

The physical security market is being enhanced through technological innovations including integrated sensors, video, and access systems. Security concerns around hardware and network infrastructure are also spurring the market to evolve. Additionally, use of the cloud and an [increase of investments](#) in hybrid solutions for real-time monitoring are triggering growth.

According to a report by [GrandViewResearch.com](#), the physical security market has been valued at USD 51.94 billion in 2013 & is likely to reach a value of USD 110.09 billion by 2020, growing at a CAGR of 11.3% from 2014 to 2020. The global physical security system market was valued at USD 51.94 billion in 2013.

" The internet of Things (IoT) continues to forge new integrations between a vast, ever-growing array of **systems, sensors, devices and services.**



With unbridled **connectivity of sensors to people, processes and things**, once disparate systems, such as physical security, will be a critical part of the IoT. "

-Security Journalist, Debora O'Mara

Physical Security

Marketplace by System



Safety and Security



Access Control



Perimeter Intrusion Detection



Screening and Scanning



Video Surveillance



Physical Security Information



The nonprofit ONVIF promotes and develops global standards for interfaces of IP-based physical security products. ONVIF Steering Committee Chair Per Björkdahl says cloud-based access control systems may be a sound place to start when updating a security system.

As we've seen everywhere, when systems have moved to the cloud, endless flexibility and scalability are the primary benefits,' says Björkdahl. "ONVIF has been 'cloud-conscious' for a while, which is why we have focused on providing standards that enable customers to deploy systems that maintain flexibility through an open interface in the cloud or on a server-based system."

When asked how much he sees the access control niche growing in the next five to 10 years, Björkdahl said: "Admit-

tedly, the speed of adoption of new technology in access control has historically been slower than it is with other physical security disciplines like video, which may have affected its growth. Access control systems can last a very long time and it's much harder to 'rip and replace' an access control system, compared with a video surveillance system. It can also be difficult to deploy a truly hybrid access control system, so many are reluctant to install new access control technologies because of compatibility issues."

That being said, the increasing demand for integrated systems along with the rise of cloud-based solutions and IoT's interconnected everything approach may very well speed up the access control industry's adoption of new technology and broaden its appeal to the market.

“Cloud computing has been around for some time now, starting with the formal public Internet in 1990. But the nature of it has changed and evolved quickly and dramatically. **Now, the cloud is becoming foundational to many emerging security applications,** including mobile credentialing involving Near Field and Bluetooth communications, with the Internet of Things (IoT) poised to come on strong as still another disruptive technology within the physical security space.”

- *Security Journalist, Deborah O'Mara*

How Should

The Physical Security Market Approach IoT

Measuring the ROI (return on investment) for physical and access security until a breach occurs is like looking for a needle in a haystack. The best way to developing a security plan of this nature is to calculate the cost of exposure.

To justify the cost of security upgrades and services, it is often necessary to assess your company's risks. Consulting firm PricewaterhouseCoopers (PwC) recommends that companies determine what their most valuable information assets are, where they are located at any given time, and who has access to them. From there, the physical security industry should collaborate with IT security departments to find a balance between protecting these assets, while developing new, smart tech enhanced services.

Cloud computing has been around for some time now, starting with the formal public Internet in 1990," says security journalist Deborah O'mara. "But the nature of it has changed and evolved quickly and dramatically. Now, the cloud is becoming foundational to many emerging security applications, including mobile credentialing involving Near Field and Bluetooth communications, with the Internet of Things (IoT) poised to come on strong as still another disruptive technology within the physical security space. - Security journalist, Deborah O'Mara

Physical security journalist Deborah O'Mara says that in spite of the fear of security breaches, companies will need to gravitate toward IoT-enabled physical security, or cloud-based access control, in order to compete and stay "future ready." They don't want to risk putting anything on their network if safeguards are not in place," says O'Mara.

" Now, the cloud is becoming foundational to many emerging security applications, including mobile credentialing involving Near Field and Bluetooth communications, with the Internet of Things (IoT) poised to come on strong as still another disruptive technology within the physical security space."

- Security journalist, Deborah O'Mara





“The physical security industry has always been concerned about breaches because of the nature of the data being communicated and followed protocols to harden products and make them less susceptible to network compromise. But now having cyber security processes and protocols is demanded by the end-user customer. They don’t want to risk putting anything on their network if safeguards are not in place.” While these safeguards are proving to be solid, there is still apprehension around IoT-enabled physical security. Bill Ho says the fear will subside over time with technological advances.

O’Mara explained that cloud-hosted access control has safeguards that button up communications between physical security products and devices. These include:

- Two-factor authentication
- AES encryption
- Secure SSL connections

“When smartphone enabled door locks became popular a few years ago, many skeptics thought it also brought additional risks like hackers unlocking your house remotely,” said Ho. “But in reality, someone who’s breaking into your house is probably finding an easier way—an open window for example. If there is fear, it’s probably with the immaturity of the IoT platforms. With the rush to internet-enable everything including toasters, security may be secondary. And once IoT devices start popping up in corporate settings, they’re another ‘hole’ that needs to be addressed from a security standpoint. I expect IoT security to improve significantly over the next few years, and we’ll most likely see some standards emerge that enable IT groups to better monitor and actively manage device security settings.”

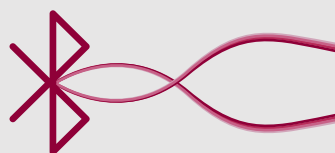
When asked if IoT-enabled physical security is cause for privacy concern, O’Mara said: “The real threat comes from all the new sensors, wearables and other items in our Bring Your Own Device society that might not have these inherent safeguards, or the communications method they are using for connectivity, such as Wi-Fi. However, the physical security industry is savvy and is working with IoT providers; a per-

fect example is the proposed BLE standard, which ultimately will foster additional integrations.”

The BLE (Bluetooth Low Energy) standard she’s referring to is being developed by the Cloud, Mobility and IoT Subcommittee Working Group of the SIA Standards Committee. [O’Mara writes](#) that the goal of the BLE standard is to “enable interoperability between mobile credentials (phones, wearables, etc.) and readers permanently affixed to physical structures. Further, a BLE standard would promote the growth and use of mobile credentials and expand the utility of access control solutions.”

Security expert Alan Silberberg of Silberberg Innovations says the convergence of IoT and physical security should begin at the foundational level of cyber security strategies.

“There is an increasing need for the combination of physical security with cyber security, and not just in IoT Devices,” said Silberberg. “The more that cyber security is embedded into the physical architecture of both chips and devices, the more that ease of use transmutes ease of not doing.” When asked what tech startups can do to obtain the best



“ However, the physical security industry is savvy and is working with IoT providers; a perfect example is the proposed BLE standard, which ultimately will foster additional integrations, ” – says O’Mara

safeguards Silberberg said: “The best cases for startups dealing with IoT security or other cyber security issues are not often shared, nor is there any standard to apply. As a result, some startups take the extra time and effort and spend the money to be secure from day one, while others do it as an afterthought or layer on top of their stack. Some startups skip security entirely in the rush to market. The best case would be a startup baking security into their devices and chips and software at the kernel levels or core layers of their stack.”

Why

IT Departments Need To Own Physical Security

For physical security to be best in class and for startups to follow best practices, physical security needs to be IoT-enabled and be operated by IT departments. Why? Physical security is comparable to a border that is locked and prevents intruders from getting through and causing harm or stealing items of value. This practice doesn't work in modern organizations. Due to the growth of the freelance and independent consultant market and the increase in collaborative projects, many workplaces today have more foot traffic than companies did decades ago.

IoT-enabled physical security, such as [smartphone managed locks](#), enable companies to treat their office entrance as an access point, where data flow. The level and type of data can also be controlled. This is the same logic that applies to monitoring internet traffic. Knowing what type of traffic comes through a company's door allows IT departments and office managers to see whether or not specific visitors should be able to log into their business's network.

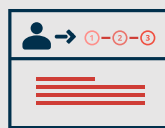
Regarding implementation, companies need to be mindful of the network an IoT device runs on, as well as who can access that network through the device. Beyond securing data, IoT-enabled physical security can provide the following.



Identity Management



Traffic Monitoring



Easy Employee On-Boarding



Improves Company Culture



Employees Don't Have To Carry Keys

These benefits create better workplaces and enhance physical and cyber security without making the work environment a prison.

Cyber Security Firms

And IoT-Enabled Physical Security

“ So the idea that the keys are virtual gives us a lot more flexibility about who we can let into our space. ”

A U.S. based cyber security firm (choosing to be anonymous) installed KISI's smart keyless system to have better data access across its three offices.

“We needed an API that would allow us to sort that data out,” said the CEO. “We make a cyber security analytics software and so we can throw it in there relatively easily. So it's much easier to manage. So I can have the front of the office managed access and not have it be required of the IT department to go in and use old school systems, and connect and add access and probation access.”

The CEO pointed out that single sign-ons for accessing a network, or having one password, has become the norm across companies.

“We kind of feel the same way about the smartphone,” said the CEO. “For most people their multi-factor is their smartphone, and it's the most important device in their life. With a smart keyless system companies can set restrictions about whether they're near the office. People like me can let them in remotely. You can require that they have to open the app so they have to know the password to their phone. So it's more secure than a key card.”

Smart keyless systems also allow executives to track when employees are traveling between offices, and see who's becoming less engaged based on the hours they're putting in or the time of day they're starting and leaving the office.

Scott Almeida, CFO of the cyber security firm Recorded Future, said deciding to outsource the company's physical security to a smart keyless provider came down to common sense.

“We have our whole product suite in the cloud, and we host it all on Amazon,” said Almeida. “When I think of the security Amazon can provide to our service, as opposed to if we tried to do it ourselves, I think, ‘it just wouldn't work.’ That's why I apply that same logic to our physical security.”

Regarding the level of security control, IoT-enabled physical security provides, Almeida said he believes Recorded Future has more control because the company can give people keys that “expire after a couple of hours.”

“If we give someone an actual key they can go out and make a copy of it in two minutes,” he explained. “So the idea that the keys are virtual gives us a lot more flexibility about who we can let into our space.”

Bringing Physical Security

Into The 21st Century

While IoT fears exist, companies that choose to remain analog in their physical security run the risk of falling prey to the pitfalls of antiquated thinking—something no tech startup wants to be known for or experience. Any networked system anywhere can get broken into at any given time. By hiring a company dedicated to managing and protecting their physical security through smart technology, startups put themselves in the best position to secure their data, and control their relationship with IoT, rather than letting the proliferation of IoT control them.

kisi



© 2016 Kisi Inc.
sales@getkisi.com
getkisi.com
646.663.4880