INDUSTRIAL INTEGRITY IN A CONNECTED WORLD

IoT, CIE, & ICS

HOW TO SUSTAIN THE INTEGRITY OF INDUSTRIAL SYSTEMS IN A CONNECTED WORLD

ZYGOTEK

Strategic Risk » Managed Outcomes

zygotek.com | info@zygotek.com | +1 (415) 376-9704

AN OVERVIEW

Security always lags behind technology adoption, and few technologies have seen growth as explosive as the Internet of Things (IoT). Security has been an afterthought until now, whe ability of the devices to connect to the internet and their widespread usage, IoT products are prime targets for hacks and IP theft or political gains. Companies have invested in IoT in the absence of robust security because of the business opportunities available.

Cisco estimates the number of connected devices will surpass 50 billion by 2020, while IDC expects that, by 2019, investments will near $1.3 trillion, vs $591.7 billion in 2014, at a CAGR of 17%. IoT security is now a strategic pillar in the digital landscape.

The industry is overdue for a new, comprehensive security model for connected devices based on network and AI. To start, altering or interrupting connected device performance alone can constitute a catastrophic breach — even one with life-or-death consequences.

What this tells us is that a vast majority of organizations today are simply unequipped and inexperienced in dealing with this exponential threat.

It's clear that significant steps need to be taken within a majority of organizations to address growing vulnerabilities as cyber attacks continue disrupting the industrial base at large.

121,588

IoT devices breached in 2018, up from 32,614 in 2017. Mirai accounted for 20.9% of breaches.

$318 billion

global IoT market growth by 2023 from $130B in 2018.

12 Million

IoT attacks with 86,560 unique IP addresses from Brazil, US, Russia, China, with malware from 27,693 unique IPs.

50%

IoT incidents where financial impact estimate has been given, have led to sizeable financial losses (>$1M)

70%

of the most commonly used IoT devices contain vulnerabilities. 56% are "unlikely or highly unlikely" to be able to detect a sophisticated attack.

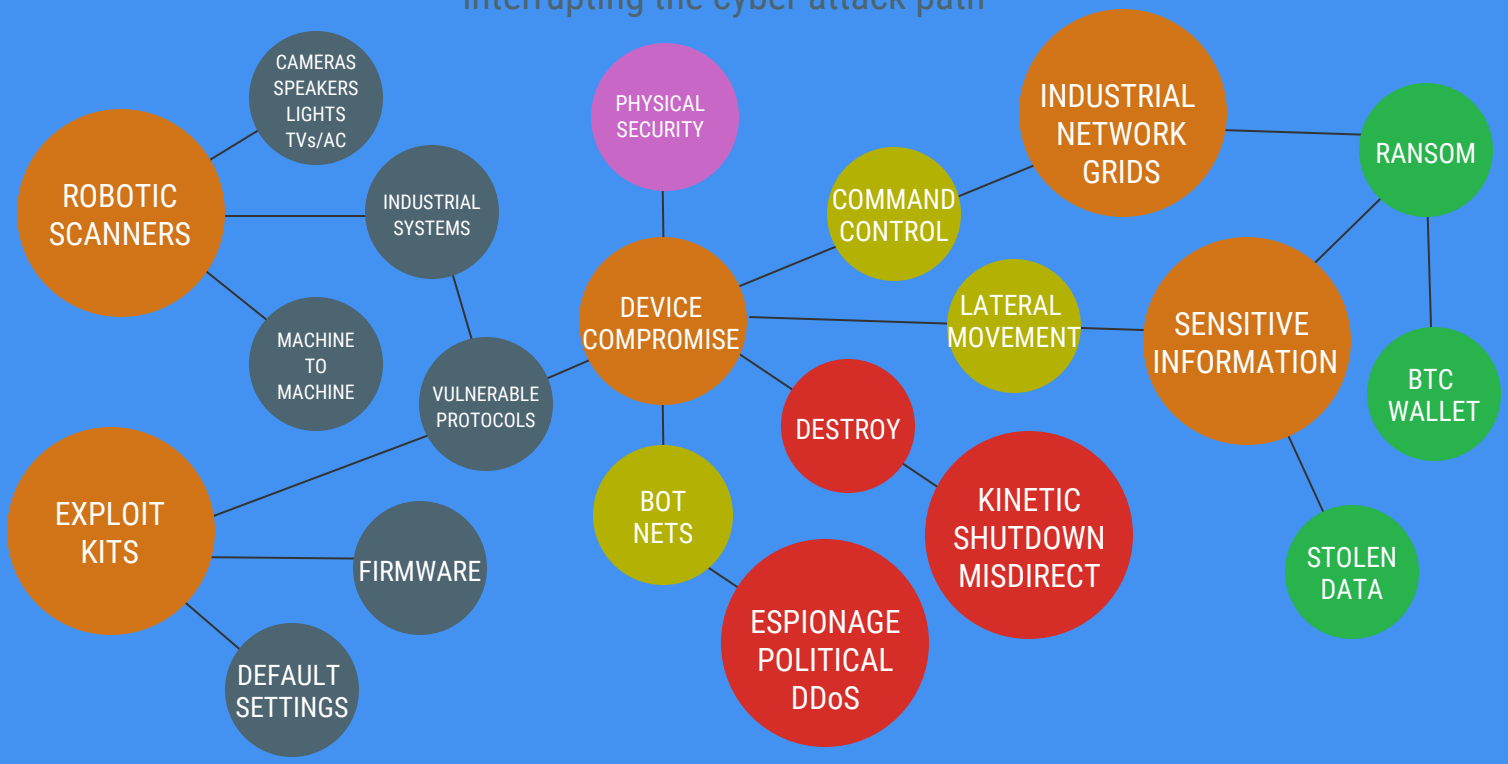
$2 Million

cost to enterprises for each IoT based DoS or DDoS attack, not counting secondary hard losses.

zygotek.com | info@zygotek.com | +1 (415) 376-9704

OUR METHODOLOGY

interrupting the cyber attack path



IDENTIFY EXPOSURES & SUSCEPTIBILITY » DETECT & PREVENT EXPLOITS / C&Cs » PREVENT PROACTIVELY & RECOVER RAPIDLY

Assess your exposures and mitigate your weaknesses

We evaluate your perimeter and internal networks, endpoints, IoT, CIE, and ICS devices, servers, and infrastructure devices looking for security weaknesses that bad actors will attempt to exploit and help you remediate the exposures.

Stay calm and be confident during a cyber crisis

Knowing what to do in the first 5 minutes of a cyber incident or data breach can save you a lot of time and money in the future. We collaborate with you on how to prevent the breach from rapidly spreading across your enterprise.

Eliminate uncertainty and recover the business quickly

We help you build, test, and implement threat intelligence programs with business recovery strategies that can be executed anytime to recovery from cyber attacks while helping you to prevent the exposures proactively and provide guidance on regulations.

zygotek.com | info@zygotek.com | +1 (415) 376-9704

WHO WE ARE

A powerful combination of CISOs, CTOs, CIOs, and experienced Consulting Partners.

The Zygotek team is different from other consulting firms because we are world-class executives who have spent time "in the trenches" mitigating risk, enabling opportunities, and delivering results for our companies.

We use specific set of proven principles and processes to collaborate with you and your team, to mitigate your risk, provide transformative insights, fast execution, and deliver the maximum business value for your investment.

WHAT WE DO

We help clients mitigate their strategic and digital risk, identify and act on strategic opportunities, drive new sources of revenue to their top line, and to reduce their bottom line costs. We deliver these results by following our simple four-phase methodology:

- Assess – Using our experience, we quickly and effectively assess your situation.
- Advise – Provide recommendations and roadmaps to get you where you need to be.
- Act - Using highly skilled small teams, we help you implement solutions with a rapid payback.
- Assure – To protect your investment, we conduct periodic reviews and recommend improvements.

"Trusted Advisor"

"Immediately became a trusted advisor and played a critical role in developing all of our InfoSec functions." -Global manufacturer

"Above and beyond"

"Tackles projects in an extremely organized and detailed manner, communicating at timely intervals, and going above and beyond to produce quality deliverables." -Consulting firm

"Value-add capabilities"

"Helped us develop and implement an enterprise security plan and transformed dysfunctional processes into value-add capabilities. They were an invaluable addition to our team." -Technology agency

Our experience includes helping numerous global companies in all verticals, including:

- Pfizer
- Moody's
- Johnson & Johnson
- Altisource
- St. Joseph Health
- CDC
- GIA
- HBO
- Molecular Devices
- ABSciex
- EDeal
- DeAnza College
- Ciba Specialty Chemicals
- GoPro
- Informatica
- Country of Santa Clara
- VMware
- Canadian Tire
- eBay

zygotek.com | info@zygotek.com | +1 (415) 376-9704