ISACA®

CYBER FUTURE: SECURITY AND PRIVACY DOOMED?

ROB CLYDE

CISM, NACD BOARD LEADERSHIP FELLOW

MANAGING DIRECTOR, CLYDE CONSULTING LLC

VICE-CHAIR, ISACA

EXECUTIVE CHAIR WHITE CLOUD SECURITY

EXECUTIVE ADVISOR TO BULLGUARD AND HYTRUST

11/30/2018

THE FUTURE: DIGITAL BY DEFAULT

NEW MANUFACTURING COMPANIES ARE REALLY SOFTWARE COMPANIES

> “**Tesla is a software company** as much as it is a hardware company”

ELON MUSK

TESLA CEO

OLD MANUFACTURING COMPANIES ARE SOFTWARE COMPANIES TOO?

Software is a core skill for General Motors

MARA BARRA

General Motors, CEO

Soon every business will be a **digital business with software at the core**

DIGITAL OUTAGES LIKE THOSE AT THE AIRLINES AND NEW YORK STOCK EXCHANGE ARE THE NEW NATURAL DISASTERS

THE WALL STREET JOURNAL.

“Failures Like the Delta Outage Are a Fact of Digital Business”

POPULAR SCIENCE

“Network Outages Like NYSE, United Airlines are the New Natural Disasters”

CNN

“British Airways Computer Glitch Causes Big Delay at Multiple Airports”

Source: http://blogs.wsj.com/cio/2016/08/09/failures-like-the-delta-outage-are-a-fact-of-digital-business/

CNN tech
EQUIFAX

INVESTMENT AND ATTENTION IMPROVING

THE PATH FORWARD

64%

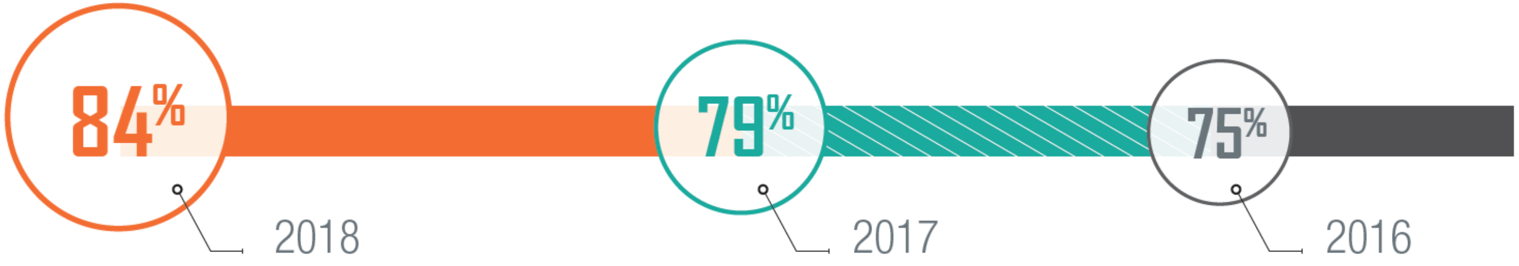
UPSWING IN INVESTMENT LEVELS:

64% indicated their security budgets would increase this year compared to **50% in 2017** and **61% in 2016**

BOARD ATTENTION:

69% say their organization's board has **adequately prioritized** information security

ALIGNING SECURITY STRATEGY WITH ORGANIZATIONAL OBJECTIVES:



Source: ISACA's State of Cybersecurity 2018

2018 STATE OF CYBERSECURITY: THREAT LANDSCAPE

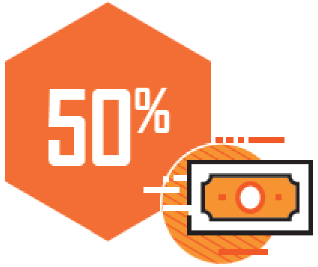
CYBERATTACKS ARE ON THE RISE AND WILL CONTINUE TO INCREASE.

50% OF RESPONDENTS

are experiencing **higher volume** of attacks this year than last year

4 IN 5

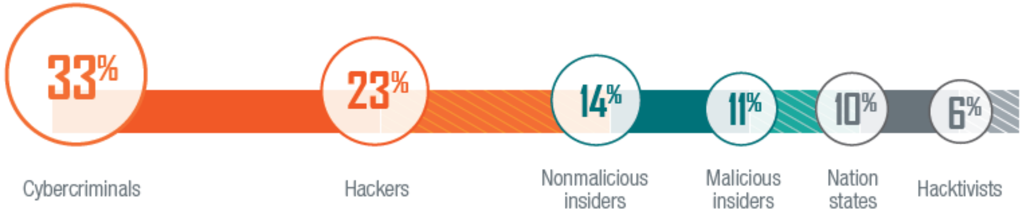
say increases **likely or very likely** to continue over the next year as well



PRIMARY MOTIVATION FOR ATTACKS:

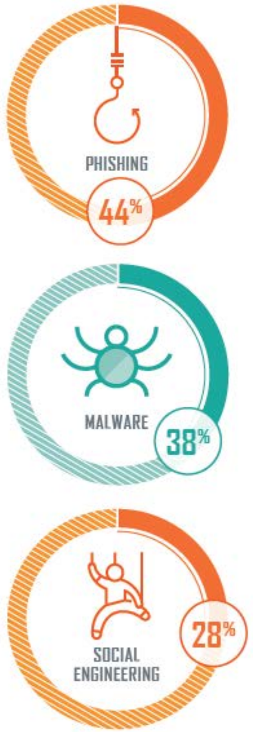
FINANCIAL GAIN

MOST COMMON TYPES OF THREAT ACTORS:



THE ATTACK

MOST COMMON VECTORS OF ATTACK:



ISACA®

RANSOMS GETTING MORE EXPENSIVE

> “Ransomware attack costs South Korean company $1M, largest payment ever”

Published June 21, 2017

Ransomware got a proverbial shot in the arm earlier this year following the WannaCry attacks and it looks as if hackers are getting more brazen with their requests as a result.

Web hosting company Nayana, based in South Korea, was attacked with the Erebus ransomware on June 10. The company ultimately had to pay a fee of 397.6 Bitcoin (approximately $1 million), the largest ransomware paid ever.

Erebus ransomware targets **vulnerable Linux servers**

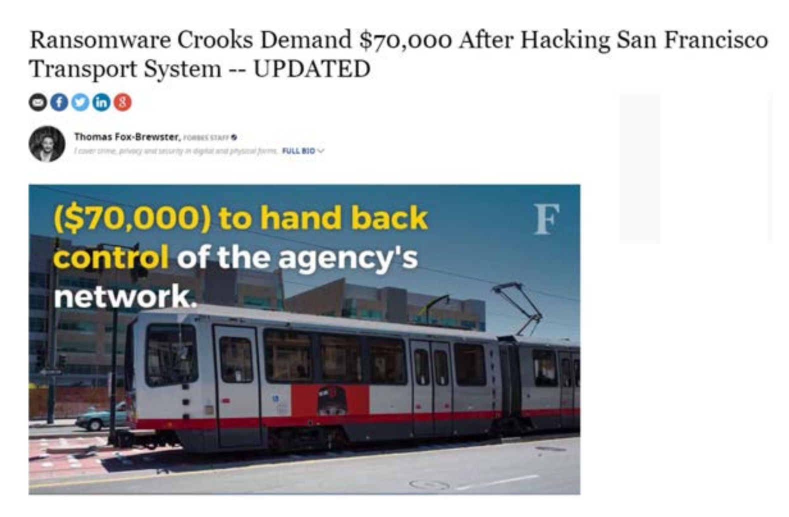
Some Nayana servers were running 2008 versions

SAN FRANCISCO TRANSPORTATION HIT WITH RANSOMWARE

CITY LETS PEOPLE RIDE FOR FREE UNTIL ISSUE RESOLVED

Forbes

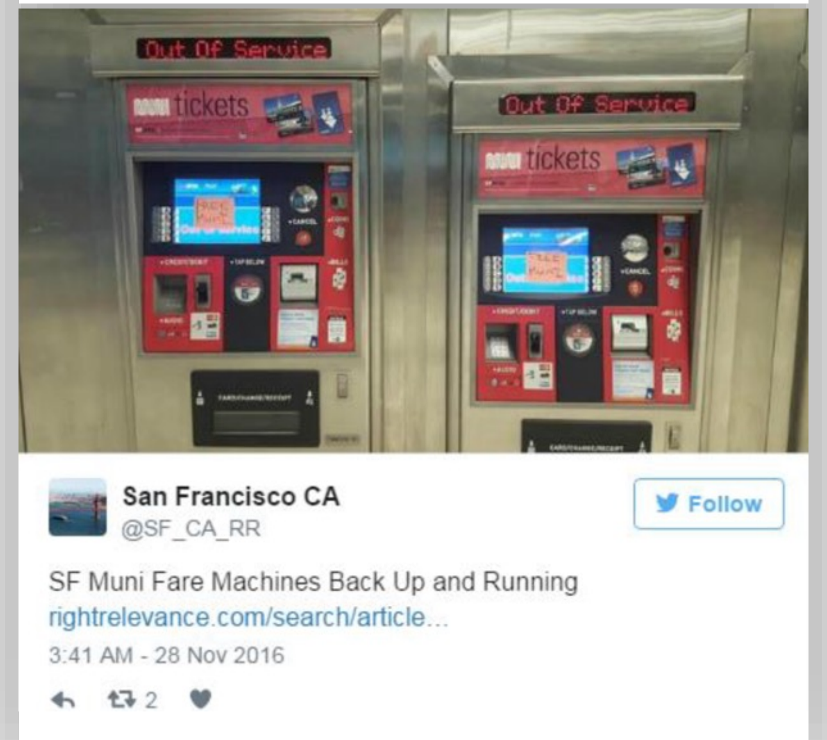
> “ Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System ”



Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System -- UPDATED

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms. FULL BIO



San Francisco CA
@SF_CA_RR

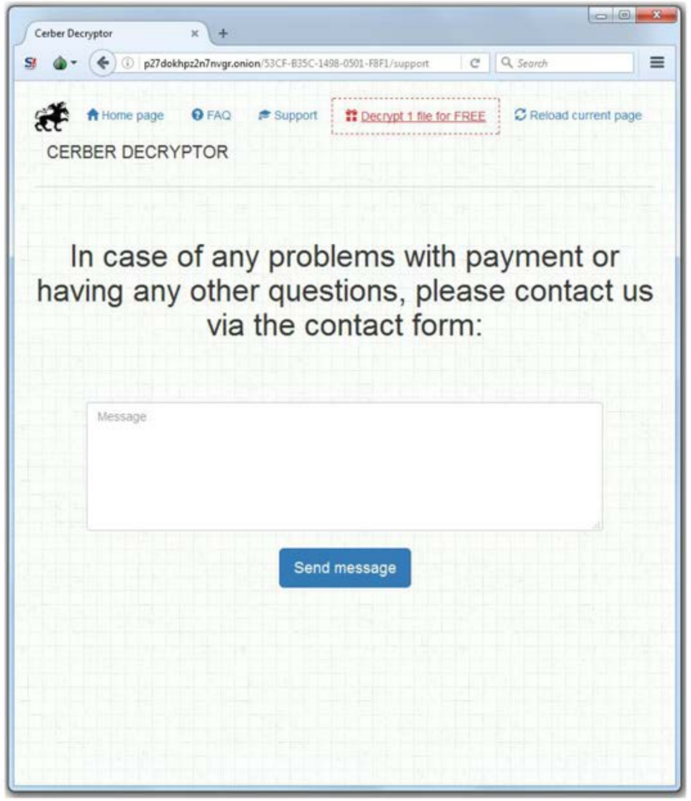
SF Muni Fare Machines Back Up and Running
rightrelevance.com/search/article...

3:41 AM - 28 Nov 2016

2

RANSOMWARE OPERATORS ADOPT TYPICAL BUSINESS PRACTICES

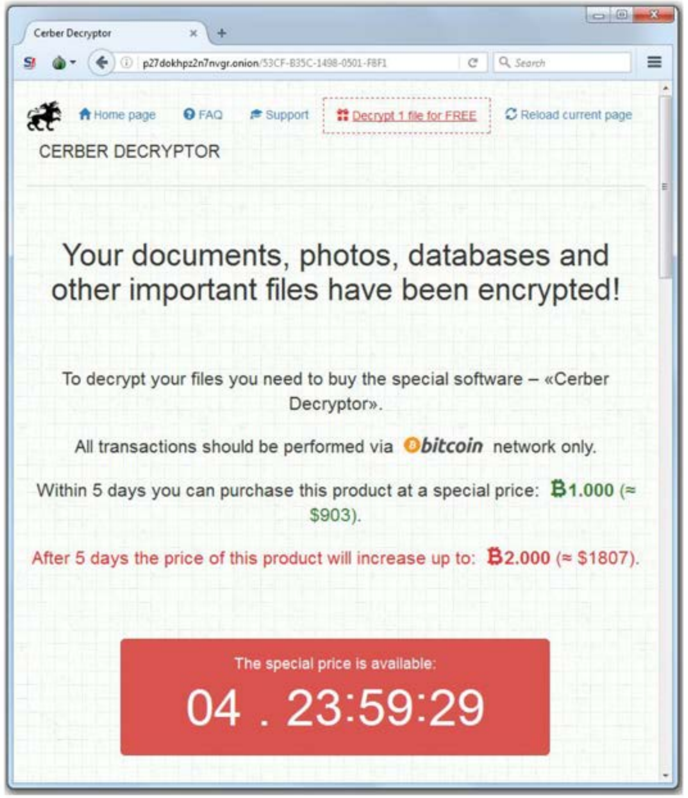
TECHNICAL SUPPORT



CERBER DECRYPTOR

In case of any problems with payment or having any other questions, please contact us via the contact form:

TIME LIMITED OFFERS



CERBER DECRYPTOR

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software – «Cerber Decryptor».

All transactions should be performed via bitcoin network only.

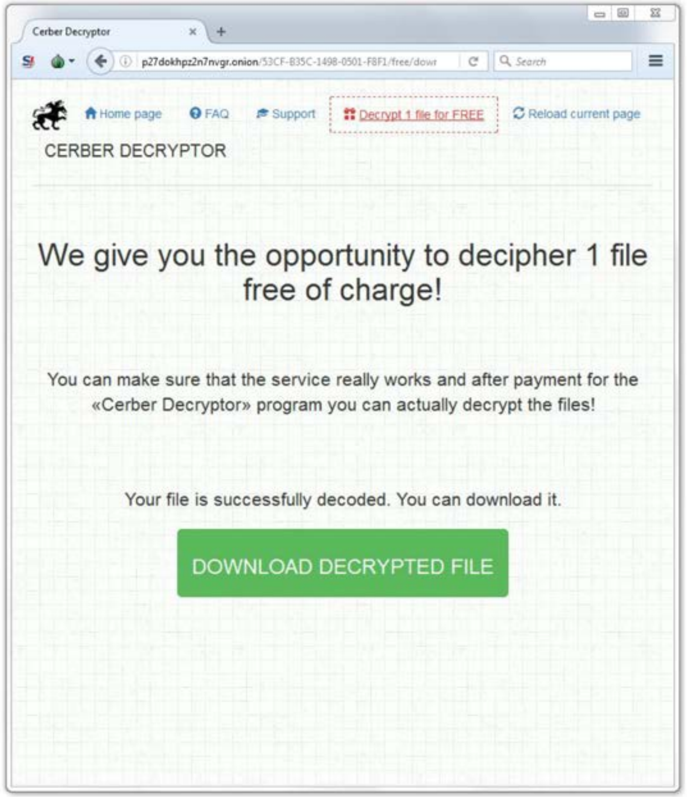
Within 5 days you can purchase this product at a special price: Ƀ1.000 (≈ $903).

After 5 days the price of this product will increase up to: Ƀ2.000 (≈ $1807).

The special price is available:

04 . 23:59:29

TRY BEFORE YOU BUY



CERBER DECRYPTOR

We give you the opportunity to decipher 1 file free of charge!

You can make sure that the service really works and after payment for the «Cerber Decryptor» program you can actually decrypt the files!

Your file is successfully decoded. You can download it.

APP CONTROL RECOMMENDED AS #1 MITIGATION STRATEGY

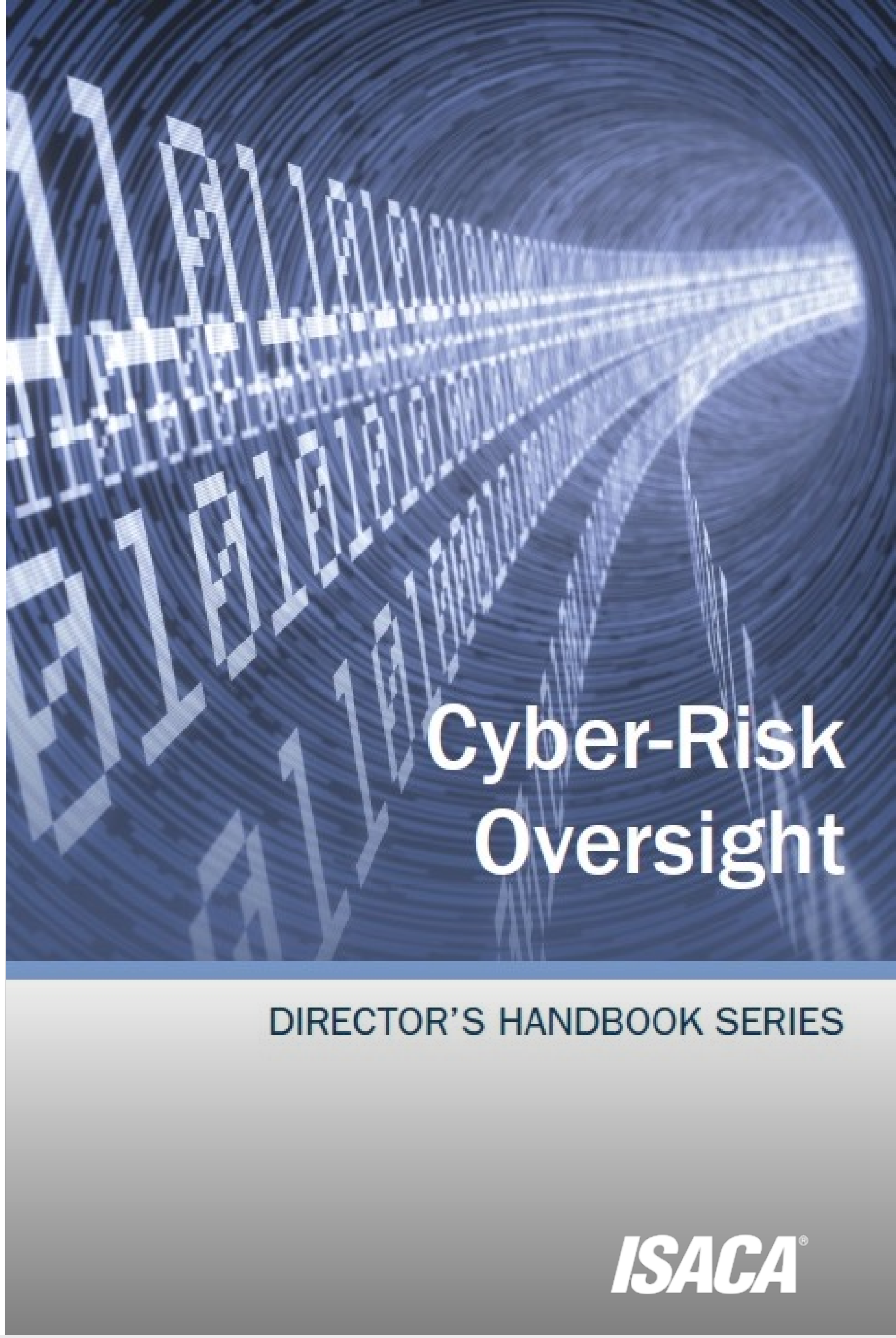
RUN ONLY KNOWN TRUSTED APPS

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

THE AUSTRALIAN GOVERNMENT

issued mandatory application whitelisting usage requirements to protect their “high value” systems

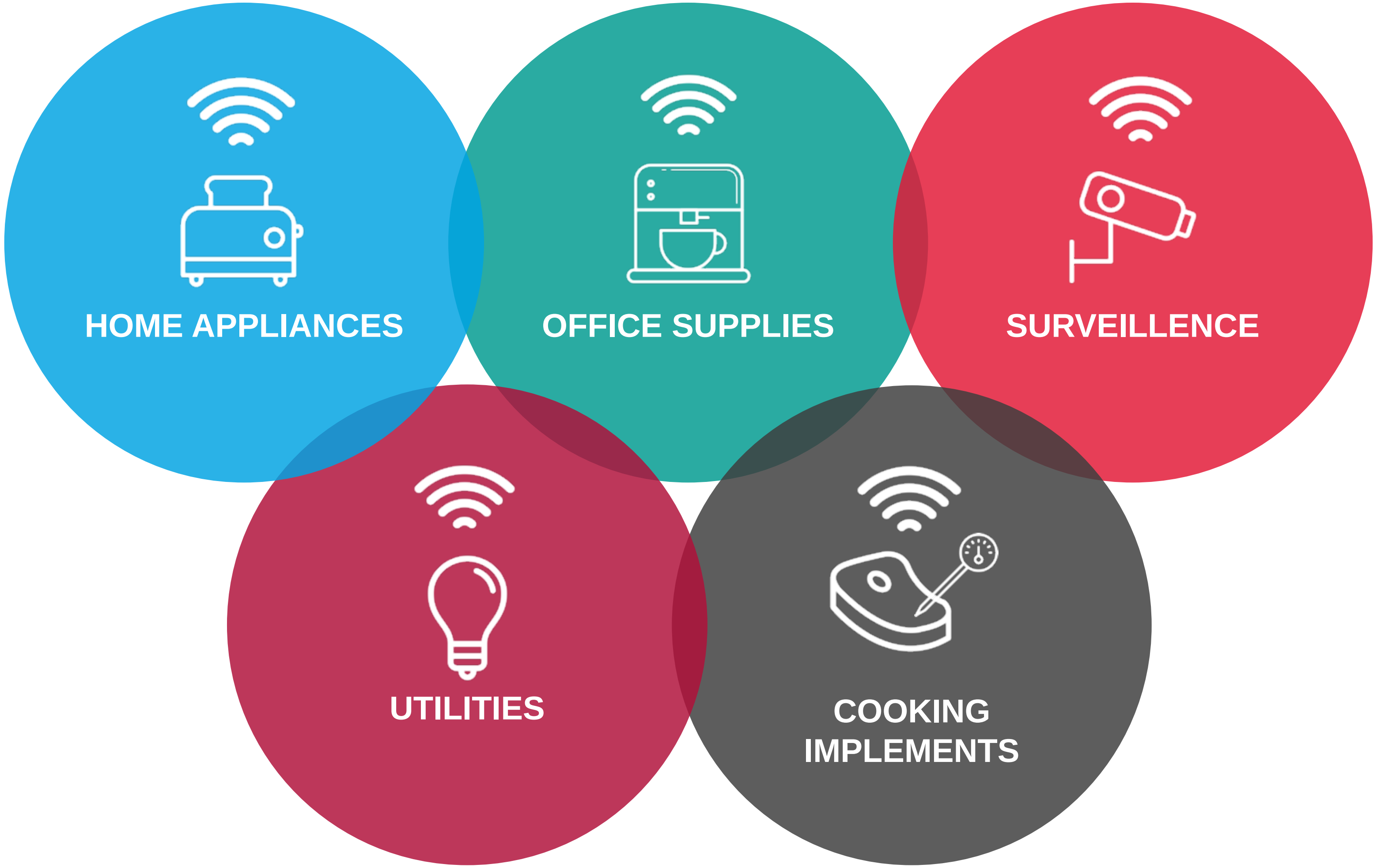


Cyber-Risk Oversight

DIRECTOR’S HANDBOOK SERIES

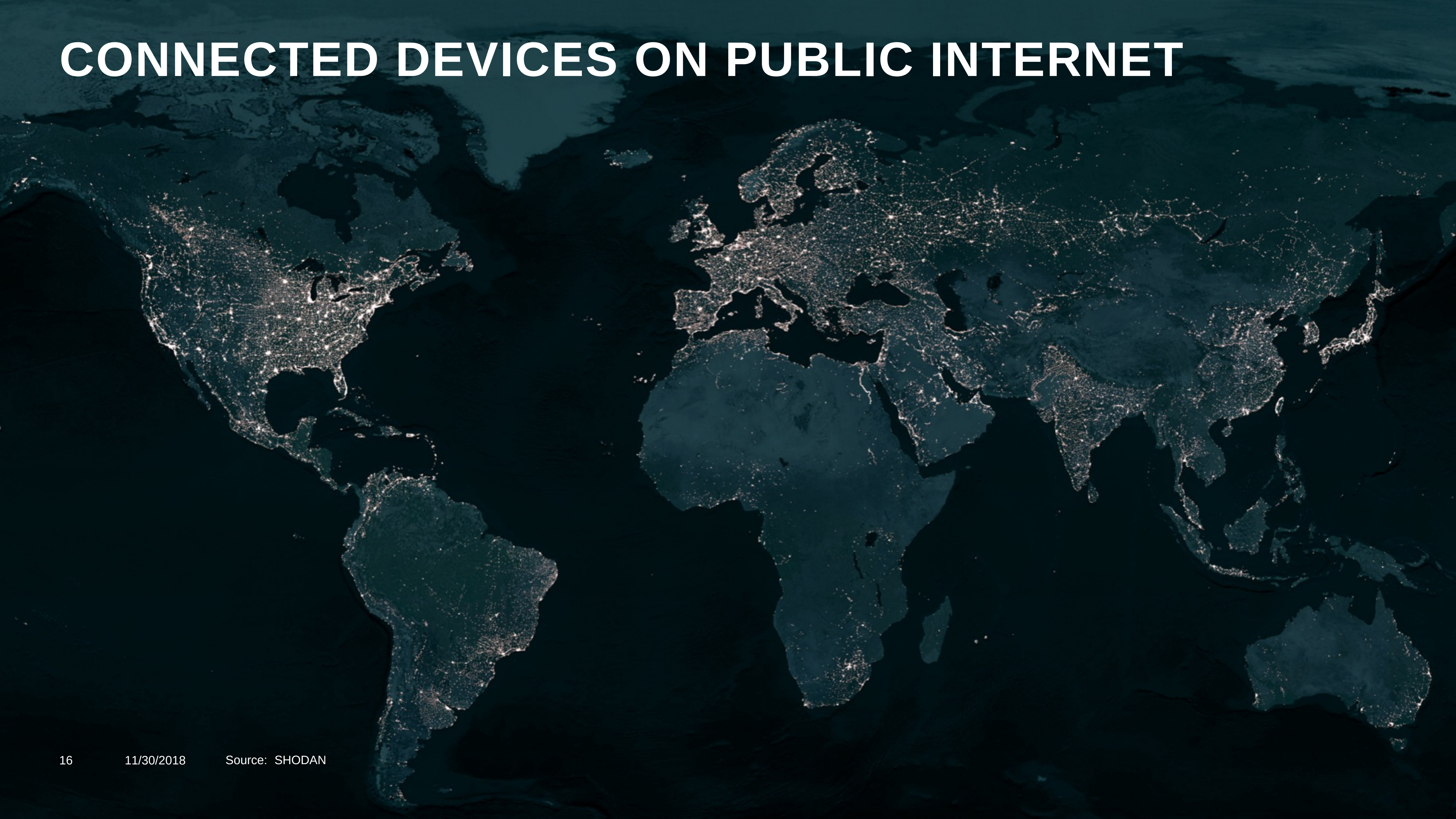
ISACA®

SOON EVERYTHING WILL BE CONNECTED



Source: https://schrier.wordpress.com/2015/05/25/the-internet-of-first-responder-things-iofrt/

CONNECTED DEVICES ON PUBLIC INTERNET



Source: SHODAN

”SMART” DEVICES ARE VULNERABLE

THE WALL STREET JOURNAL.

“Hackers Infect Army of Cameras, DVRs for Massive Internet Attacks”

Hacking shows vulnerability of internet devices, security experts say.

Attackers used an army of hijacking security cameras and video records to launch several massive internet attacks last week, prompting fresh concern about the vulnerability of millions of ”smart” devices in homes and business connected to the internet.

USING THE INTERNET OF THINGS TO SPY?

theguardian

“US Intelligence Chief: We Might Use the Internet of Things to Spy On You”

“In the future, intelligence services might use the internet of things for identification, surveillance, monitoring, location tracking and targeting for recruitment”, says James Clapper, US director of national intelligence.

Photograph Source: Alex Brandon/AP

INTERNET-CONNECTED SURVEILLANCE?

The New York Times

> “WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents”

WikiLeaks released thousands of documents that it said described sophisticated software tools used by the Central Intelligence Agency to break into smartphones, computer and even internet-connected televisions.

If the documents are authentic, as appeared likely at first review, the release would be the latest coup for the anti-secrecy organization and a serious blow to the C.I.A.

Source: https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html

INTERNET-CONNECTED SURVEILLANCE?

THE WALL STREET JOURNAL.

“China’s Tech Giants Have a Second Job: Helping Beijing Spy on Its People”

Tencent and Alibaba are among the firms that assist authorities in hunting down criminal suspects, silencing dissent and creating surveillance cities

https://www.wsj.com/article_email/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284-lMyQjAxMTI3MzA2MTIwNjE0Wj/?mg=prod/accounts-wsj

SMART THERMOSTAT VULNERABILITY

NETWORKWORLD

> “Industrial monolith sold hackable thermostats, says expert”

Thermostat program could give a potential robber times when the home may be empty.

Malicious attack could be launched by raising temperatures too high or low. Winter-time damage could include freezing, burst water pipes.

CONNECTED CARS ALSO AT RISK

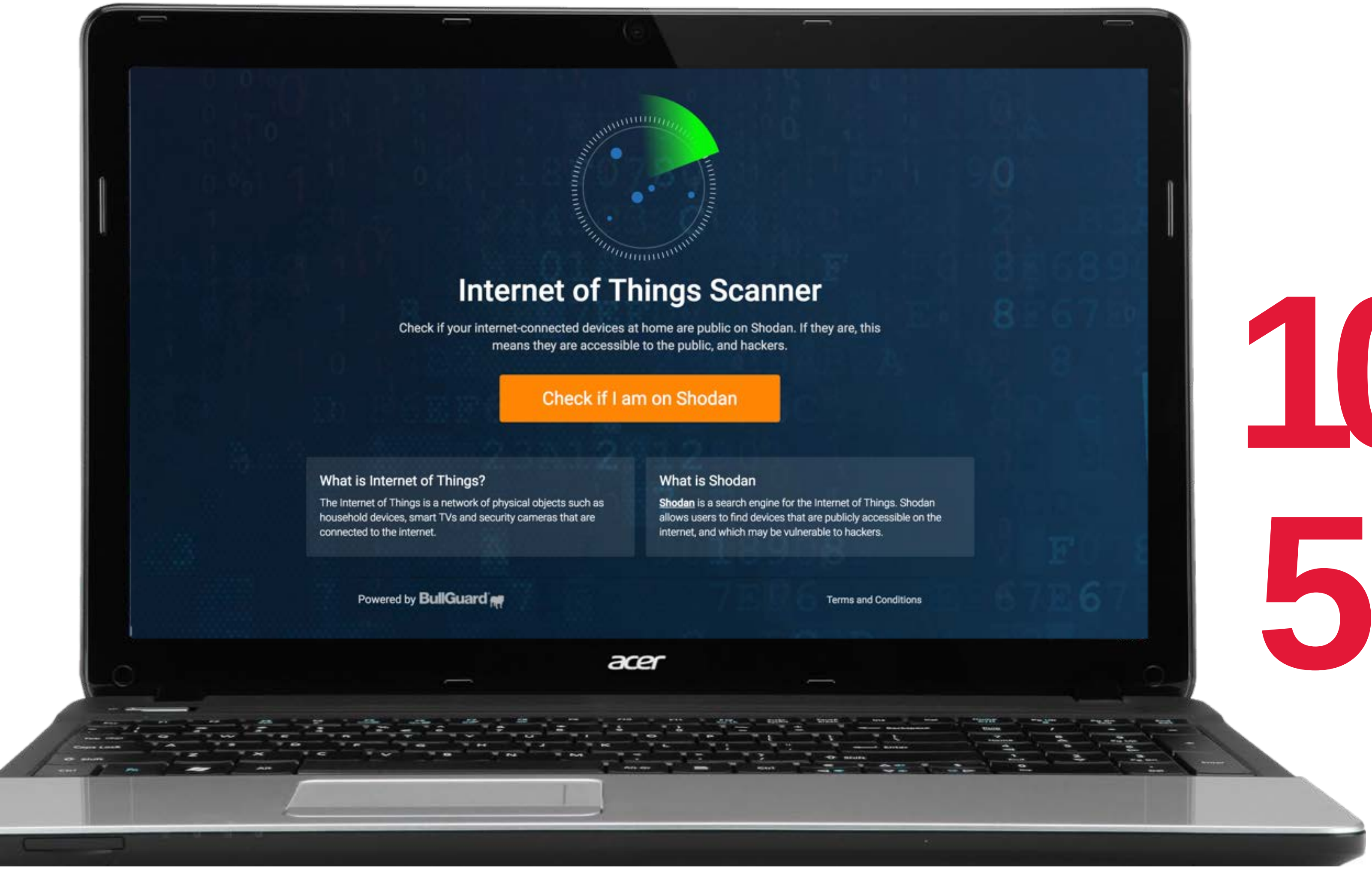
NETWORKWORLD

> “Researchers Remotely Hack Tesla Model S While it’s Being Driven”

The remote hacks likely work on all Tesla models, but on the parked Model S P85, the researchers remotely opened the sunroof, turned on the turn signal, and changed the position of the driver’s seat.

Researchers also hacked a 75D model while it was moving, controlling the brakes from 12 miles away.

IOTSCANNER.BULLGUARD.COM



Internet of Things Scanner

Check if your internet-connected devices at home are public on Shodan. If they are, this means they are accessible to the public, and hackers.

What is Internet of Things?

The Internet of Things is a network of physical objects such as household devices, smart TVs and security cameras that are connected to the internet.

What is Shodan

Shodan is a search engine for the Internet of Things. Shodan allows users to find devices that are publicly accessible on the internet, and which may be vulnerable to hackers.

Powered by BullGuard

Terms and Conditions

100K+ UNIQUE SCANS PER WEEK

5% OF SCANS HAVE VULNERABILITIES

IOT – RECOMMENDATIONS FOR ORGANIZATIONS

Safely embrace Internet of Things devices in the workplace to **keep competitive advantage**

Require wireless IoT devices be connected through the workplace **guest network or other isolated segment**, rather than internal network

Ensure all workplace devices owned by organization are **updated quickly when security upgrades are released**

Scan networks for IoT devices; **monitor for and block dangerous traffic** to or from IoT devices

Ensure **default passwords are changed** and strong

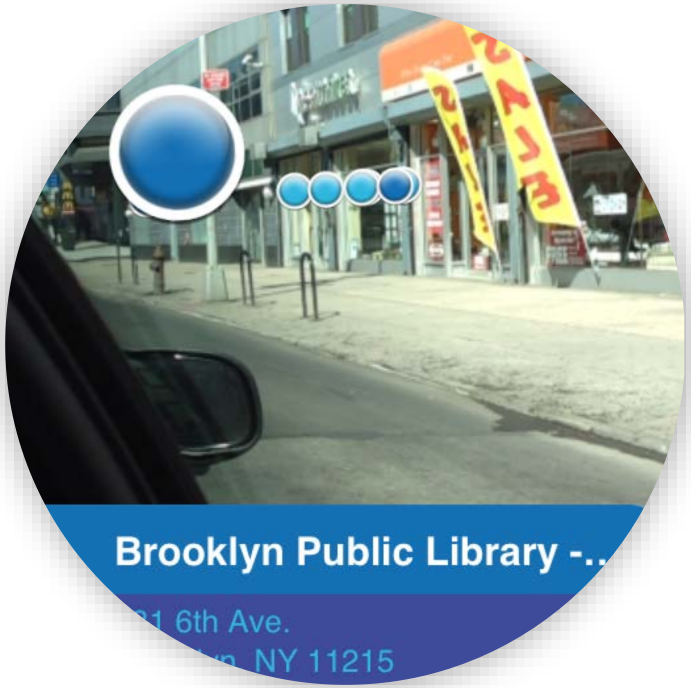
Provide **cybersecurity training** for all employees to demonstrate their awareness of best practices of cybersecurity and the different types of cyberattacks

Ensure that IT and security professionals are **ISACA certified**

AUGMENTED REALITY DISRUPTING THE WAY WE SEE THE WORLD

OPENING UP NEW WAYS OF ATTRACTING CUSTOMERS AND DOING BUSINESS

POKÉMON GO



LAYAR

COCA-COLA

BUT THERE IS A DARK SIDE TO AUGMENTED REALITY

DISTRACTED WALKING AND DRIVING

ASSOCIATES SOCIAL MEDIA INFORMATION WITH LOCATION

SHOWS POSTED, GEOTAGGED RACY IMAGES AND VIDEO

CRIMINALS USE AUGMENTED REALITY TO LURE VICTIMS TO LOCATION

GANGS AND TERROR GROUPS VIRTUALLY MARK TERRITORY AND TARGETS

AUGMENTED REALITY OPPORTUNITY AND CHALLENGES

87% Say organizations should be concerned about AR privacy risks

64% Don’t have policy to address the use of AR apps in the workplace

75% Have a way to detect pictures, posts and videos geotagged to their business locations or advertisements

AR offers the potential of positive business impact in:

NEW BUSINESS MODELS/OFFERINGS

BETTER COLLABORATION

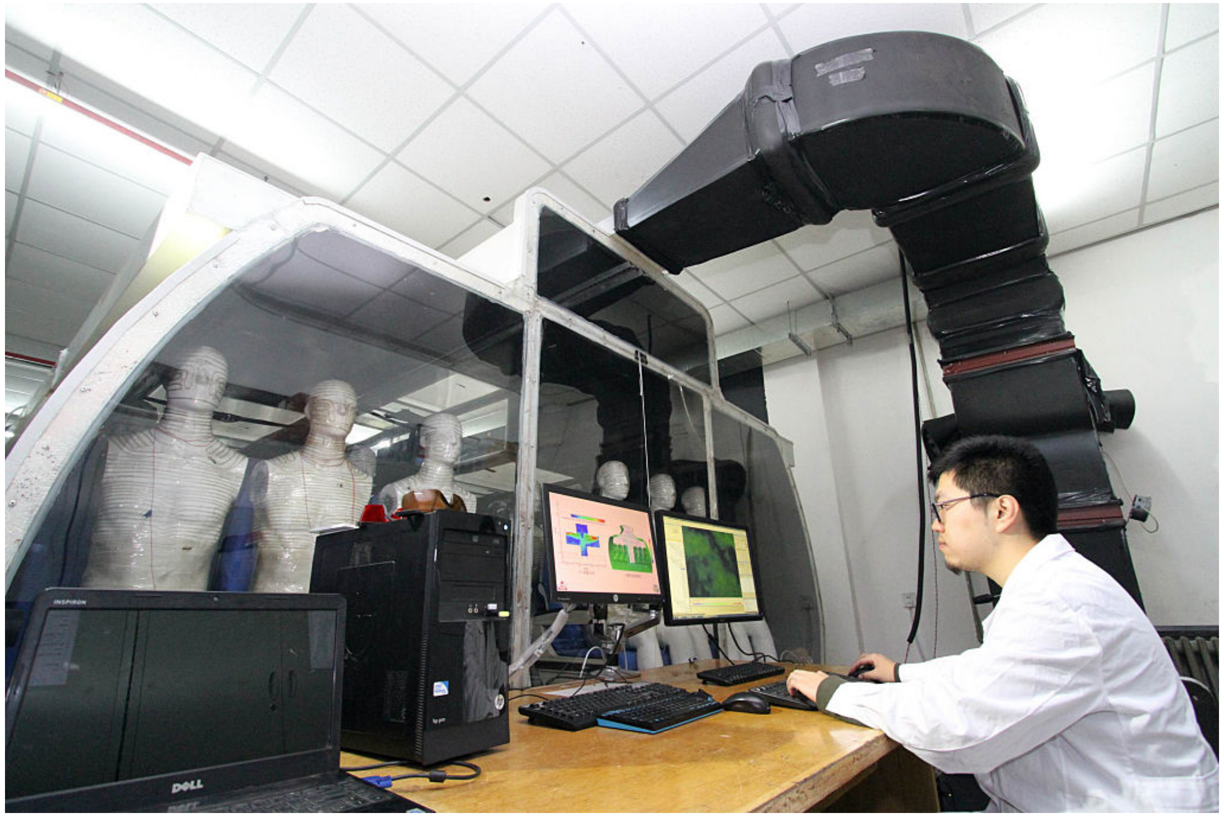
BETTER MARKETING

INCREASED EFFICIENCY

Source: ISACA Risk Reward Barometer – Nov. 2016

EVEN GENE EDITING IS DIGITAL

Chinese scientists use US-invented CRISPR/cas9 Gene editing tool in trials to cure cancer



THE WALL STREET JOURNAL.

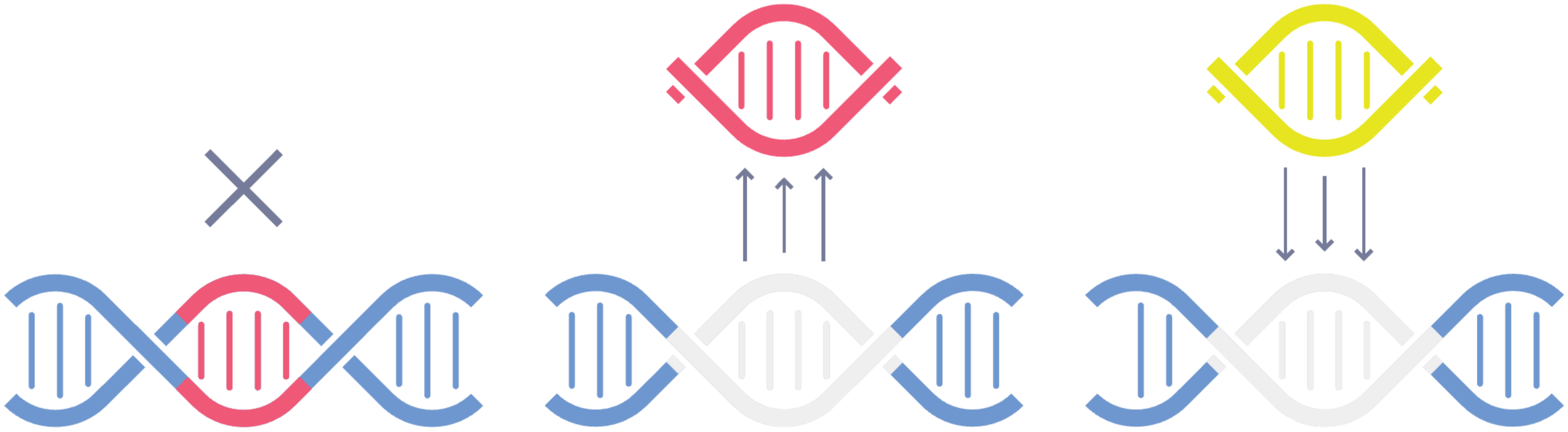
Chinese Scientist Claims World's First Genetically Modified Babies

Scientific community expresses alarm, warning that experiments using nascent DNA-editing technology pose too many risks

Gene-editing tools such as Crispr-Cas9, which Dr. He said he used, are cheap, easy-to-use and powerful. . . .

Editing so-called germ cells—the genes of sperm, eggs and embryos—is even more controversial because any changes would pass on to future generations, giving a tiny blip potentially far-reaching consequences. . . .until Monday no one has been known to have implanted them into a woman's womb.

WHAT IS THE CYBER RISK FOR GENE EDITING TOOLS LIKE CRISPR/CAS9?



DISRUPT

If a single cut is made, a process called non-homologous end joining can result in the addition or deletion of base pairs, disrupting the original DNA sequence and causing gene inactivation

DELETE

A larger fragment of DNA can be deleted by using two guide RNAs that target separate sites. After cleavage at each site, non-homologous end joining unites the separate ends, deleting the intervening sequence

CORRECT OR INSERT

Adding a DNA template alongside the CRISPR/Cas9 machinery allows the cell to correct a gene, or even insert a new gene, using a process called homology directed repair

Source: http://www.crisprtx.com/gene-editing/crispr-cas9

Cloud enables the

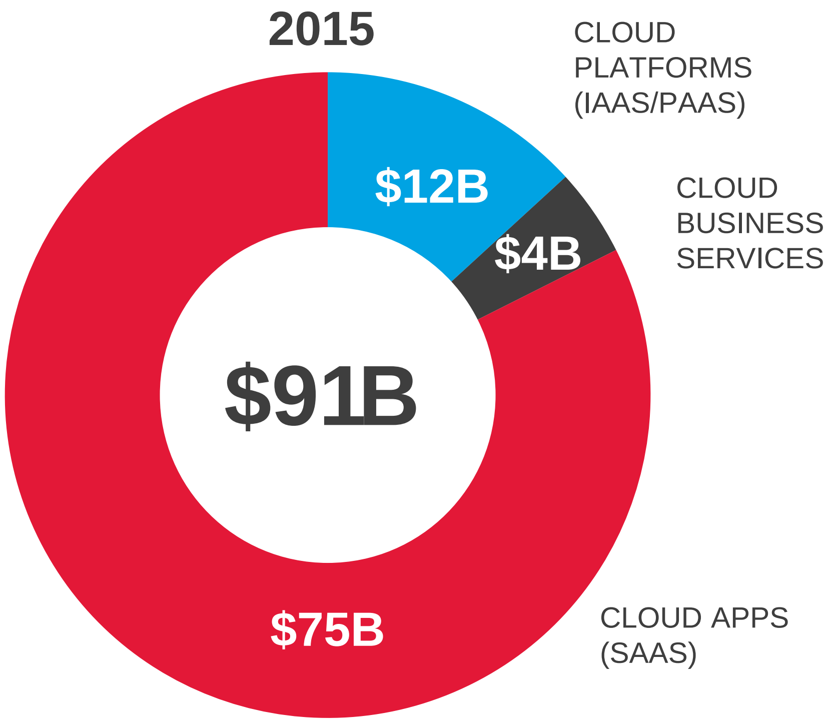
DIGITAL BUSINESS

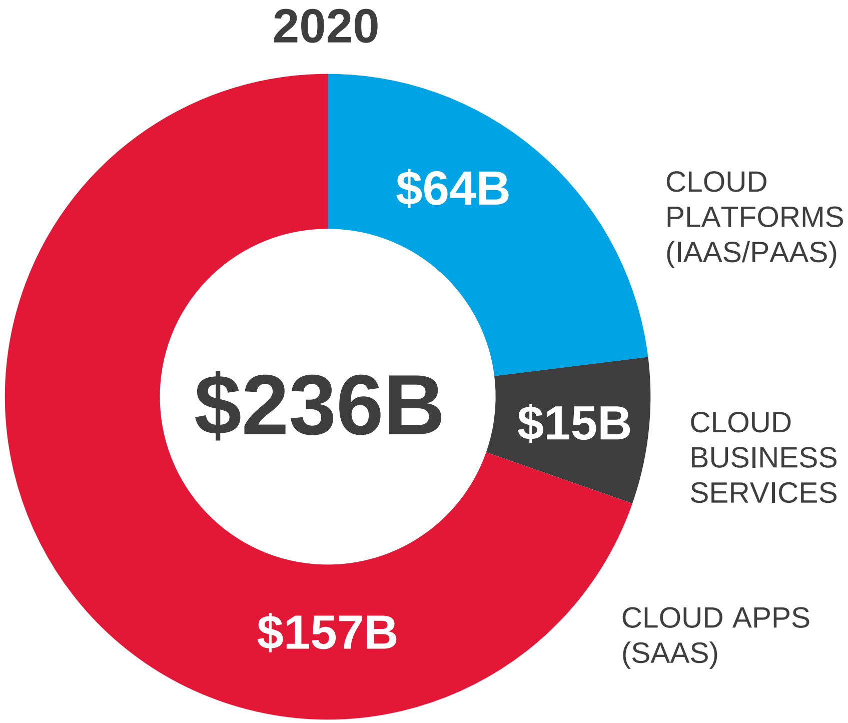
CLOUD – ALL YOU NEED IS AN IDEA AND A CREDIT CARD

One thing to **play with it.**
Another thing to **depend on it**

Reintroduce **control** without reintroducing **friction**

PUBLIC CLOUD MARKET IS IN HYPER GROWTH





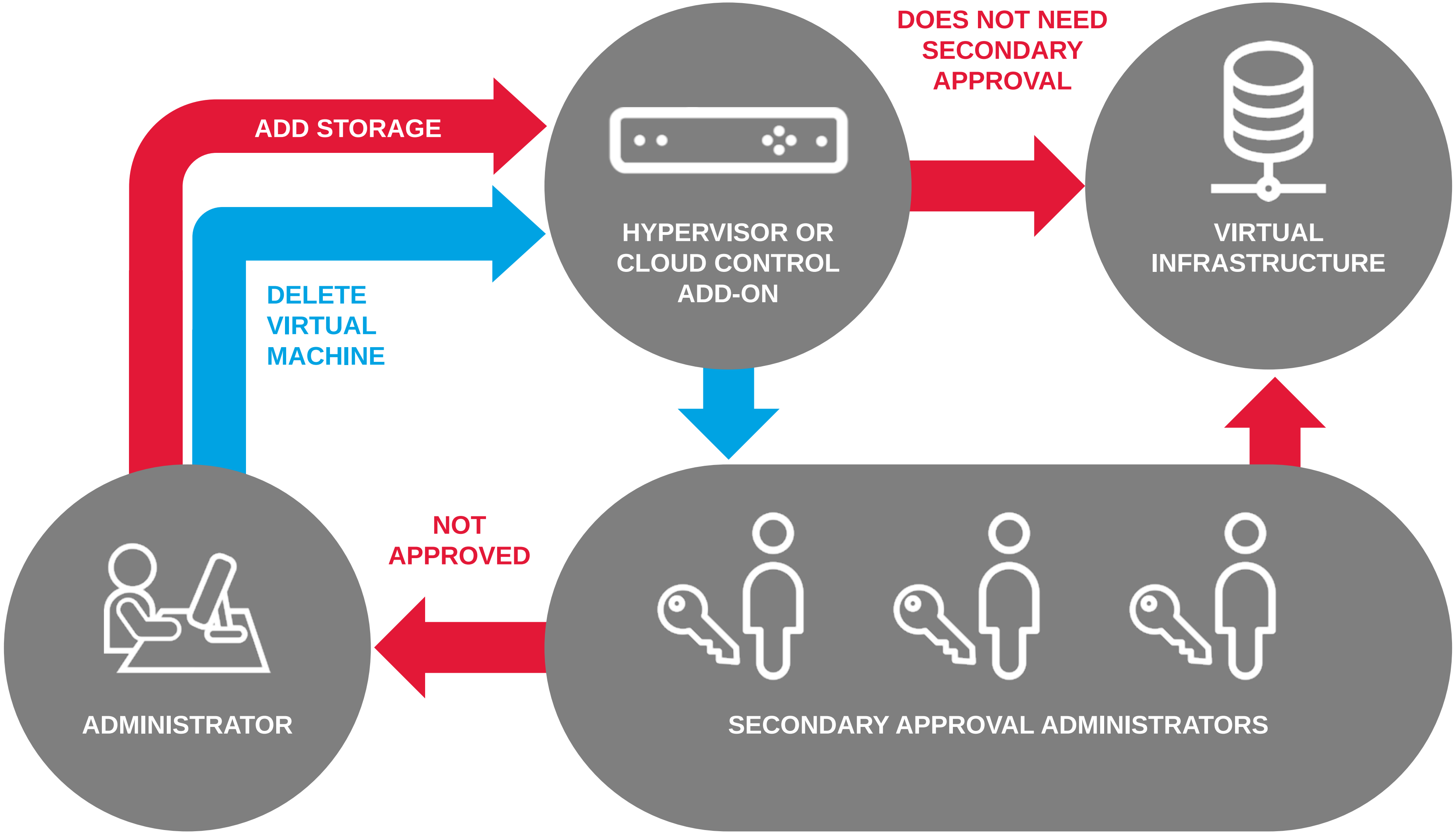
Source: Forrester, “The Public Cloud Services Market Will Grow Rapidly To $236 Billion in 2020”

WHAT LIMITS CLOUD ADOPTION?

What factors are **limiting your adoption** of virtual/private, community and public clouds today?

- Encryption helps, but key **management is critical**
- Regulatory, sensitivity and privacy issues may require that some data is **restricted to certain physical locations**
- Restrict sensitive workloads (e.g., PCI) to **trusted hardware and software** server stack
- **Only allow certain workloads** to run on hardware in approved physical location
- Only allow certain workload data to be decrypted **in approved physical location**
- Cloud solutions require **a combination of capabilities** to achieve “defense in depth” and compliance readiness

CONSIDER ADDING SECONDARY APPROVAL CONTROLS


ADD STORAGE
DELETE VIRTUAL MACHINE
HYPERVISOR OR CLOUD CONTROL ADD-ON
DOES NOT NEED SECONDARY APPROVAL
VIRTUAL INFRASTRUCTURE
NOT APPROVED
ADMINISTRATOR
SECONDARY APPROVAL ADMINISTRATORS

BIG DATA AND ANALYTICS APPLICATIONS

PREDICTING CONSUMER BEHAVIOR

CURING CANCER

PREDICTING WEATHER

REDUCING ENERGY COSTS

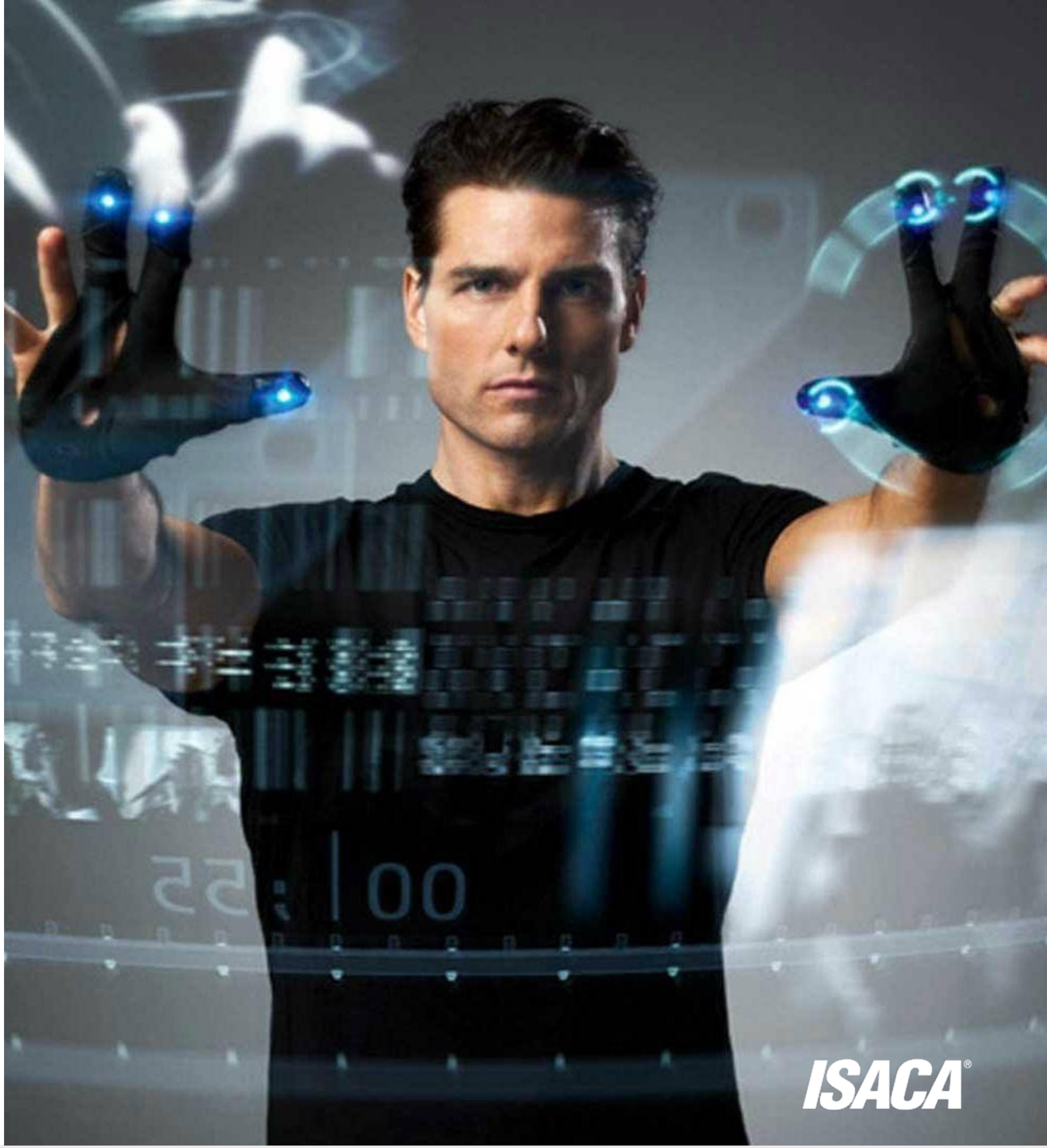
BUILD BETTER CARS

SERCURITY INTELLIGENCE AND FRAUD DETECTION

100

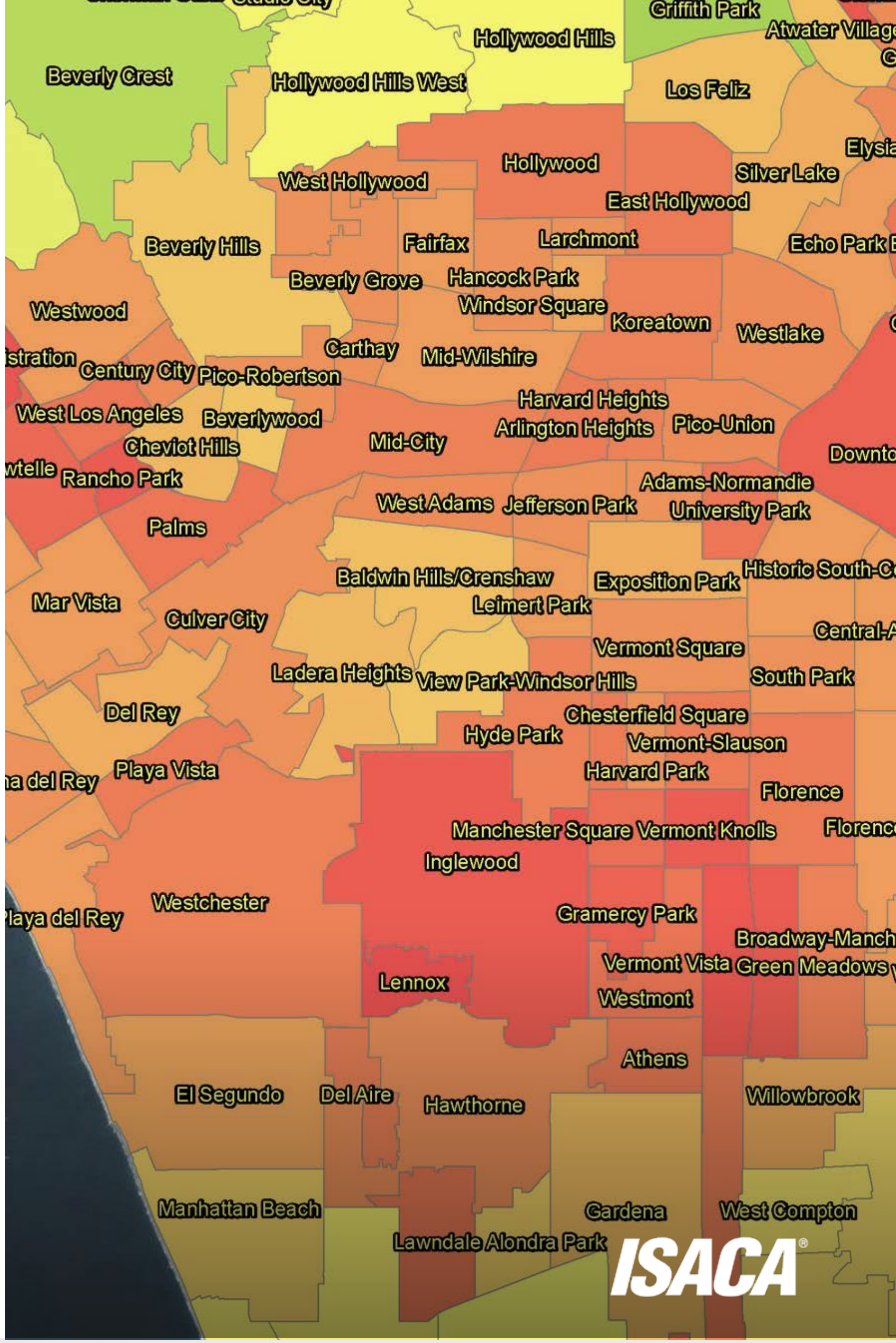
ZETTABYTES BY 2025!

What about predicting crime by particular individuals? Will we have predictive capabilities **LIKE THOSE IN THE MOVIE MINORITY REPORT, BUT THROUGH BIG DATA?**



USING BIG DATA TO PREDICT CRIME

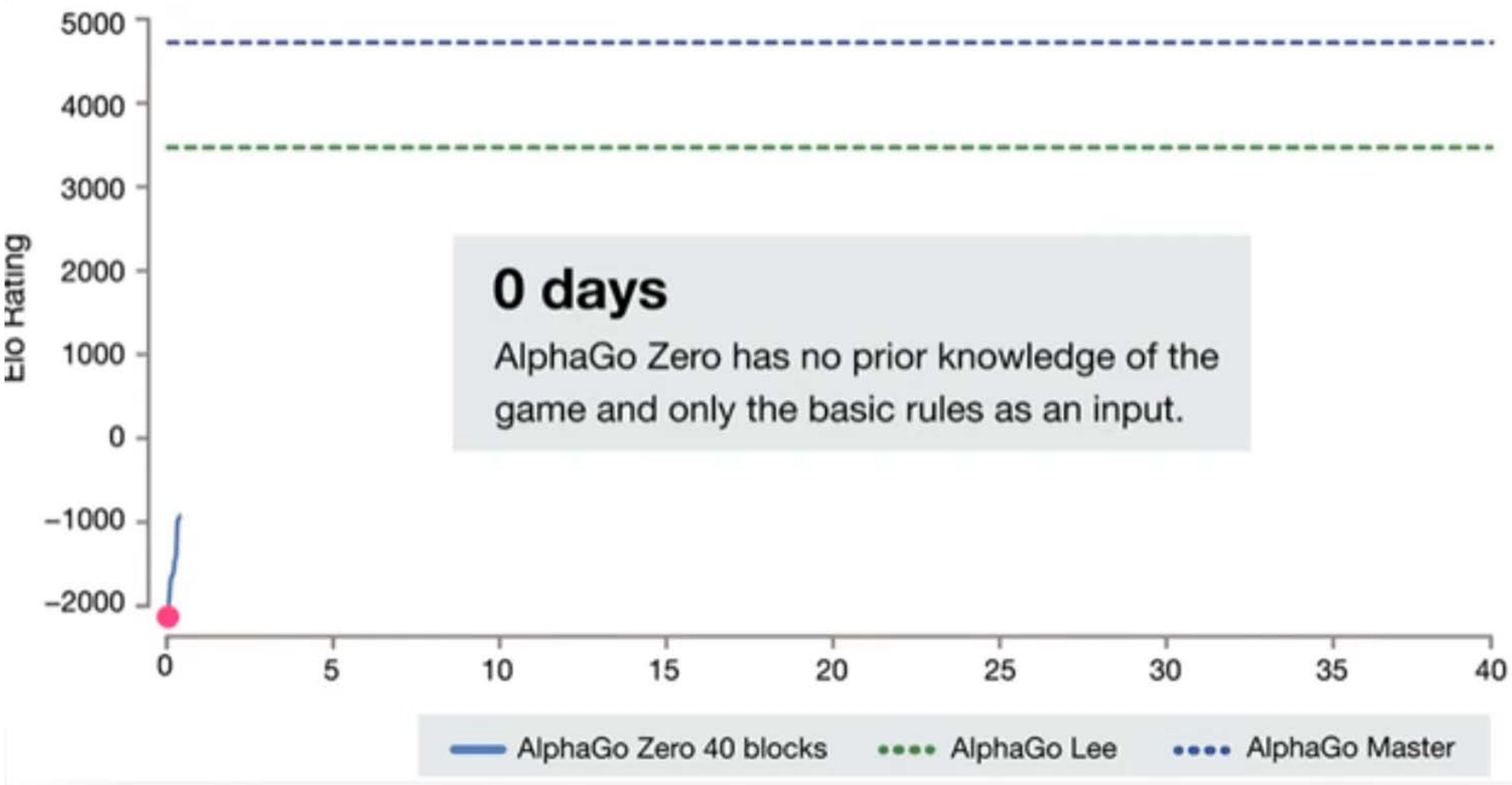
A “predictive policing” trial in California was able to identify areas where crime will occur three times more accurately than existing methods of forecasting



Source: NetworkWorld, Sep 20, 2014

PRODUCER: DAGOGO ALTRAIDE

ALPHAGO ZERO SURPASSES ALL PREVIOUS VERSIONS WITHOUT HUMAN INPUT



0 days

AlphaGo Zero has no prior knowledge of the game and only the basic rules as an input.

Source: DeepMind

DARPA CYBER GRAND CHALLENGE AT DEFCON

7 TEAMS

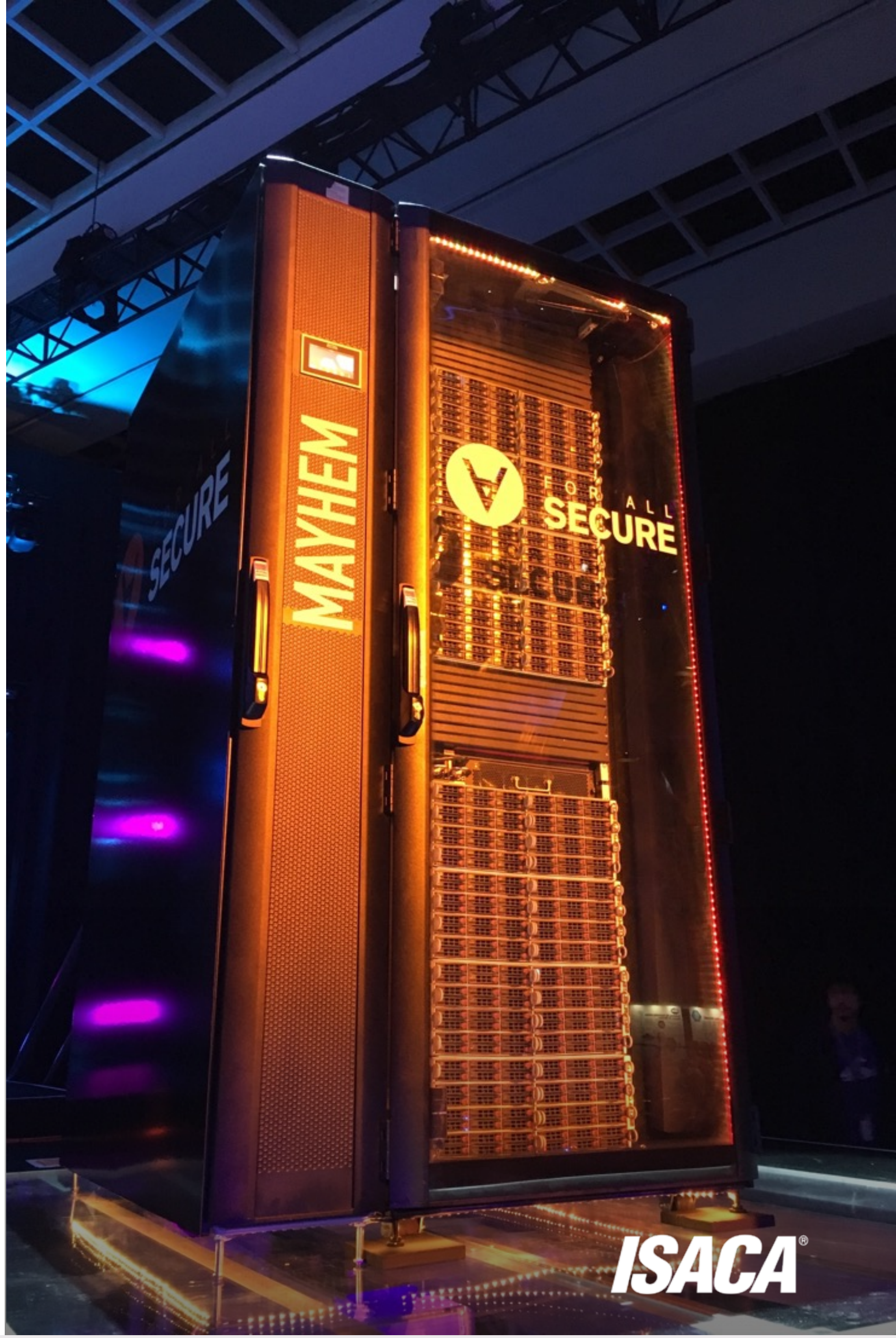
competing with individual supercomputers with machine learning programs

ATTACKING

other systems and **defending your own**

"MAYHEM"

took the top prize of $2M



Global AI experts sound the alarm

Leading researchers co-author unique report warning of the malicious use of AI in the coming decade

https://www.cam.ac.uk/Malicious-AI-Report

?

IS THE FUTURE OF **HACKING** AI?

?

IS THE FUTURE OF **CYBER DEFENSE** AI?

THE FUTURE: DIGITAL BY DEFAULT

PRIVATE AND SAFE?

QUESTIONS?

ROB CLYDE

CISM, NACD Board Leadership Fellow

Vice-Chair, ISACA International

Executive Chair, Board of Directors, White Cloud Security

Managing Director, Clyde Consulting LLC

Executive Advisor to Bullguard and Hytrust

rclyde@isaca.org

EMAIL
info@isaca.org

WEBSITE
www.isaca.org