PMP Briefing

An analysis of the current threat landscape and upcoming security challenges

Ilias Chantzos | Senior Director Government Affairs EMEA & APJ

The Big Numbers

Symantec

Web Threats

More than 1 Billion
Web requests analyzed each day
Up 5% from 2016

1 in 13
Web requests lead to malware
Up 3% from 2016

Email

Percentage Spam Rate

2015	2016	2017
53%	53%	55%

IoT

600%
Increase in Attacks

2016	2017
6K	50K

Vulnerabilities

Overall increase in reported vulnerabilities **13%**

Malware

92%
Increase in new downloader variants

80%
Increase in new malware on Macs

8,500%
Increase in coinminer detections

Ransomware

5.4B
WannaCry attacks blocked

46%
Increase in new ransomware variants

Mobile

Number of new variants

2016	2017
17K	27K

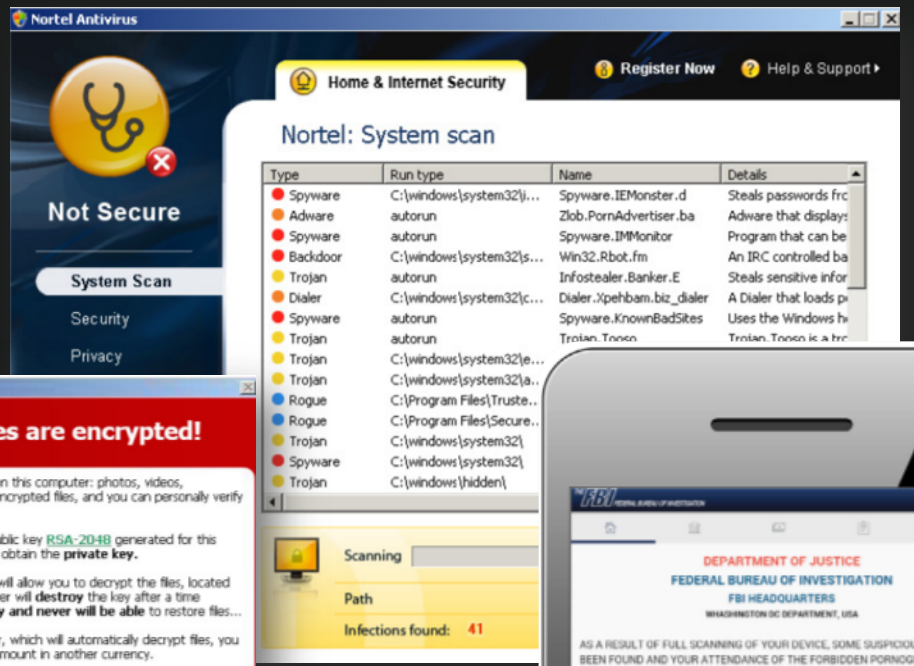
Increase in mobile malware variants **54%**

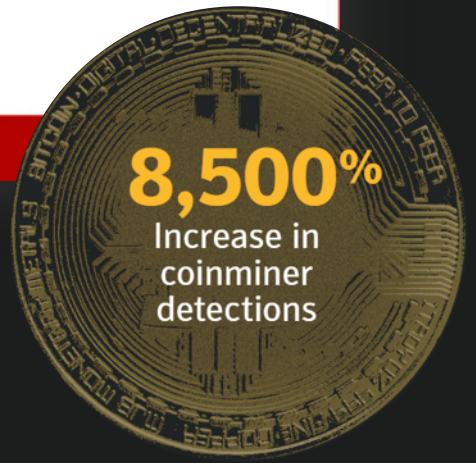
24,000 Average number of malicious mobile apps blocked each day

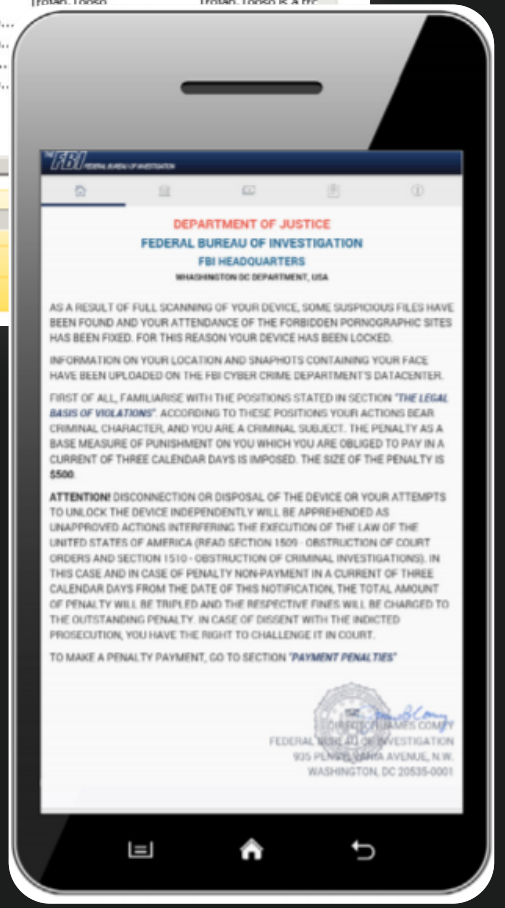
29%
Increase in industrial control system (ICS) related vulnerabilities

 |

Get Rich Quick Schemes







The Great Privacy Awakening

Trump Campaign Consultants Cambridge Analytica Found Guilty of Breaking Data Laws

DAILY BEAST

Smart gadgets open door to stalking and abuse, say police

THE TIMES

Dutch Petition Against Google's Location Tracking Gets 50,000 Signatures

NL TIMES.NL

Apple FaceTime bug lets people eavesdrop on your iPhone or Mac without your knowledge

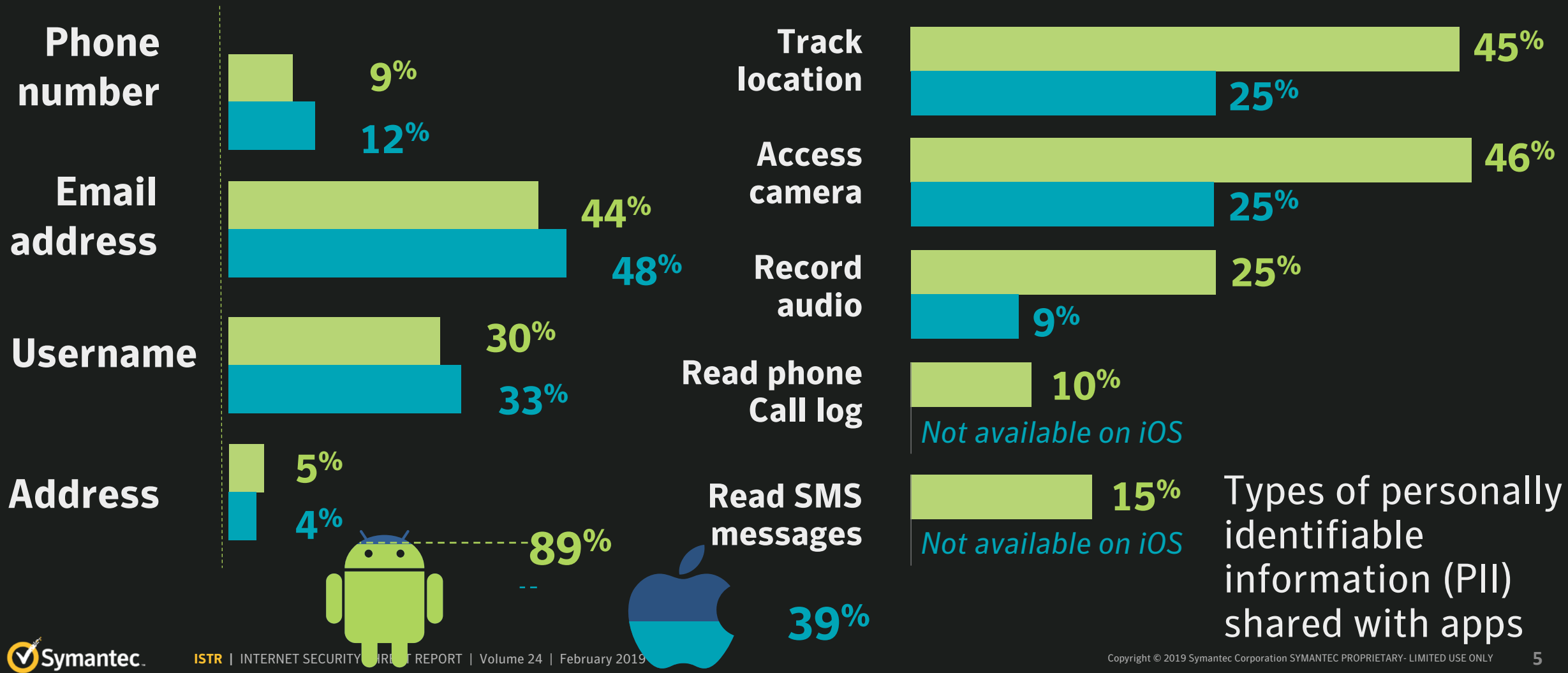
USA TODAY

Security News This Week: Employees May Have Snooped On Ring Security Camera Feeds

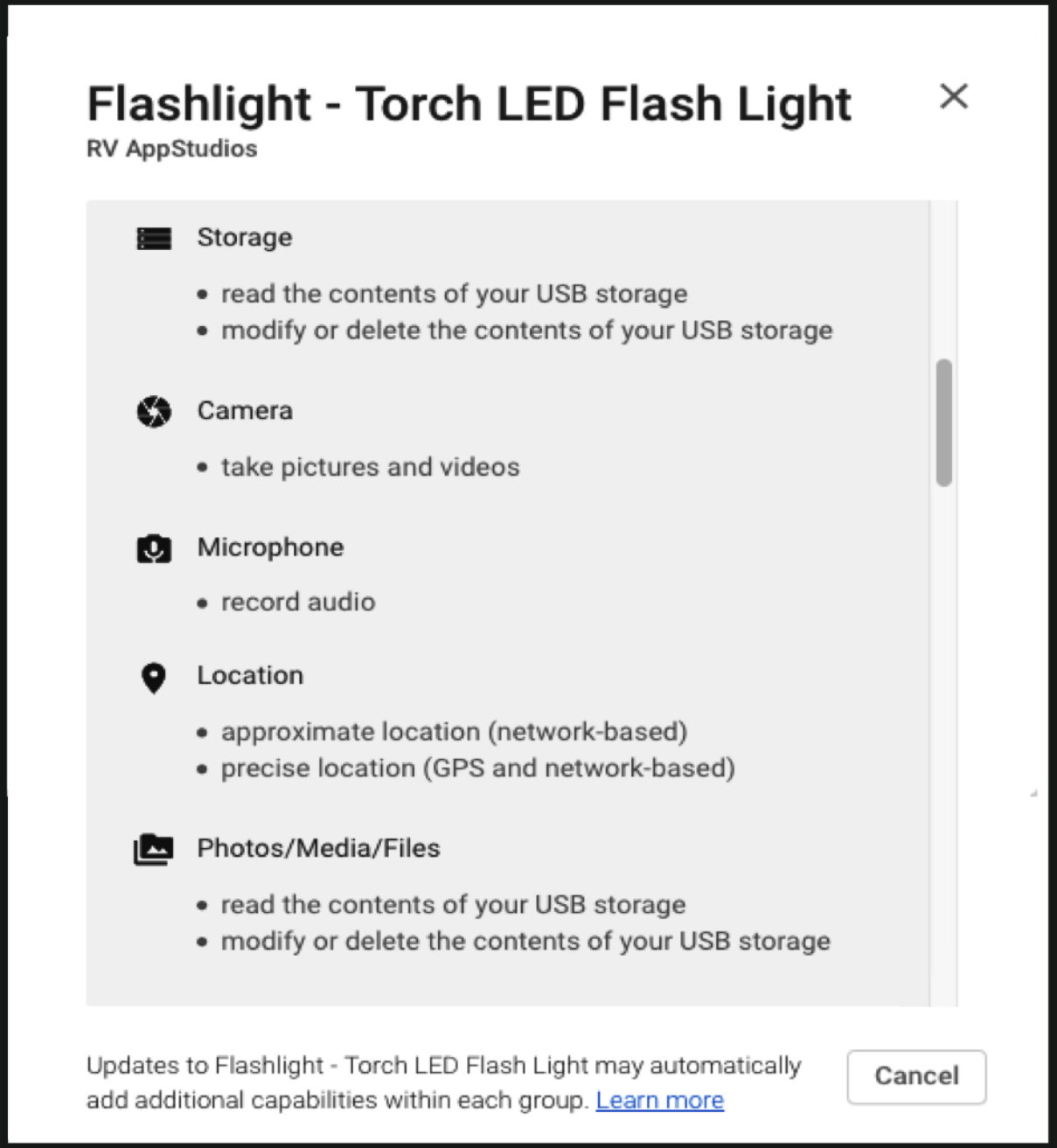
WIRED

Smartphones Are Arguably the Greatest Spying Devices Ever Created

Analysis of top 100 free apps for iOS and Android



Types of personally identifiable information (PII) shared with apps



Investor Insights

Alternative data to drive your investment models

As a hedge fund or financial manager, you want to make investment decisions

From the 200 M downloads of our flagship weather apps and 90 percent

provide the insight needed to make critical investment decisions by gauging a company's financial health before it's reflected in quarterly income statements.

Building the Models

We provide the historical foot traffic data indices you need to build a baseline footfall vs. revenue model. Then, we provide daily, weekly, or monthly normalized foot traffic data on any of IBM's large and growing library of companies. Run your model to give you a unique edge to guide your investment decisions before the rest of the market reacts.

Market Differentiators

Our true differentiators come from the scale and first-party consistency of our location data, the transparent customer terms used in its collection and use, and IBM's well-earned reputation for ethical data governance. Investor Insights provides you with the highest quality alternative data you need to run profitable investment models. The potential advantages are endless.

Using Footfall Patterns to Inform Investment Decisions

- We measure foot traffic at venue-based company locations.
- You compare this data to the company's financial performance.
- You forecast its financial health before public disclosures.
- You make investment decisions with increased confidence.

From the 200M downloads

...and 90% adoptions rate

...we collect 120M "ping" locations daily

Using Footfall Patterns to Inform Investment Decisions

- We measure foot traffic at venue-based company locations.
- You compare this data to the company's financial performance.
- You forecast it's financial health before public disclosures.
- You make investment decisions with increased confidence.

Symantec.

ATTACKS INVOLVING CONNECTED CAMERAS UP FROM 3.5% IN 2017 TO 15% IN 2018

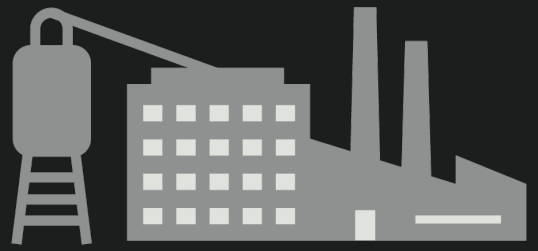
ROUTERS AND CONNECTED CAMERAS WERE THE MAIN SOURCE OF IOT ATTACKS ACCOUNTING FOR OVER 90 PERCENT

OF ACTIVITY.

IOT DEVICES EXPERIENCE AN AVERAGE OF 5,200 ATTACKS PER MONTH

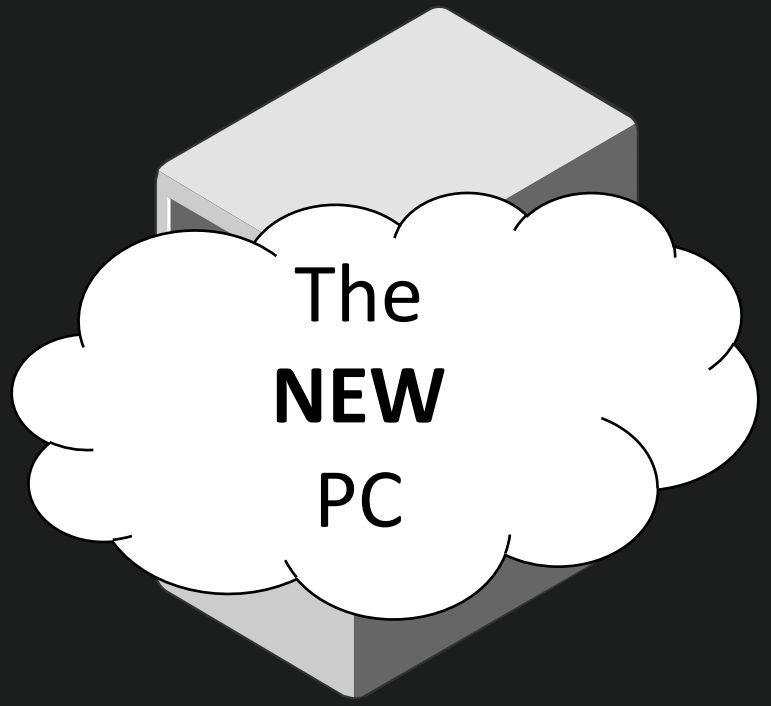
IoT an Entry Point for Targeted Attacks

A new breed of persistent, destructive IoT threat conducting MITM attacks and targeting SCADA



When it Comes to Security, the Cloud Is the New PC

The risks of cloud computing are becoming clear

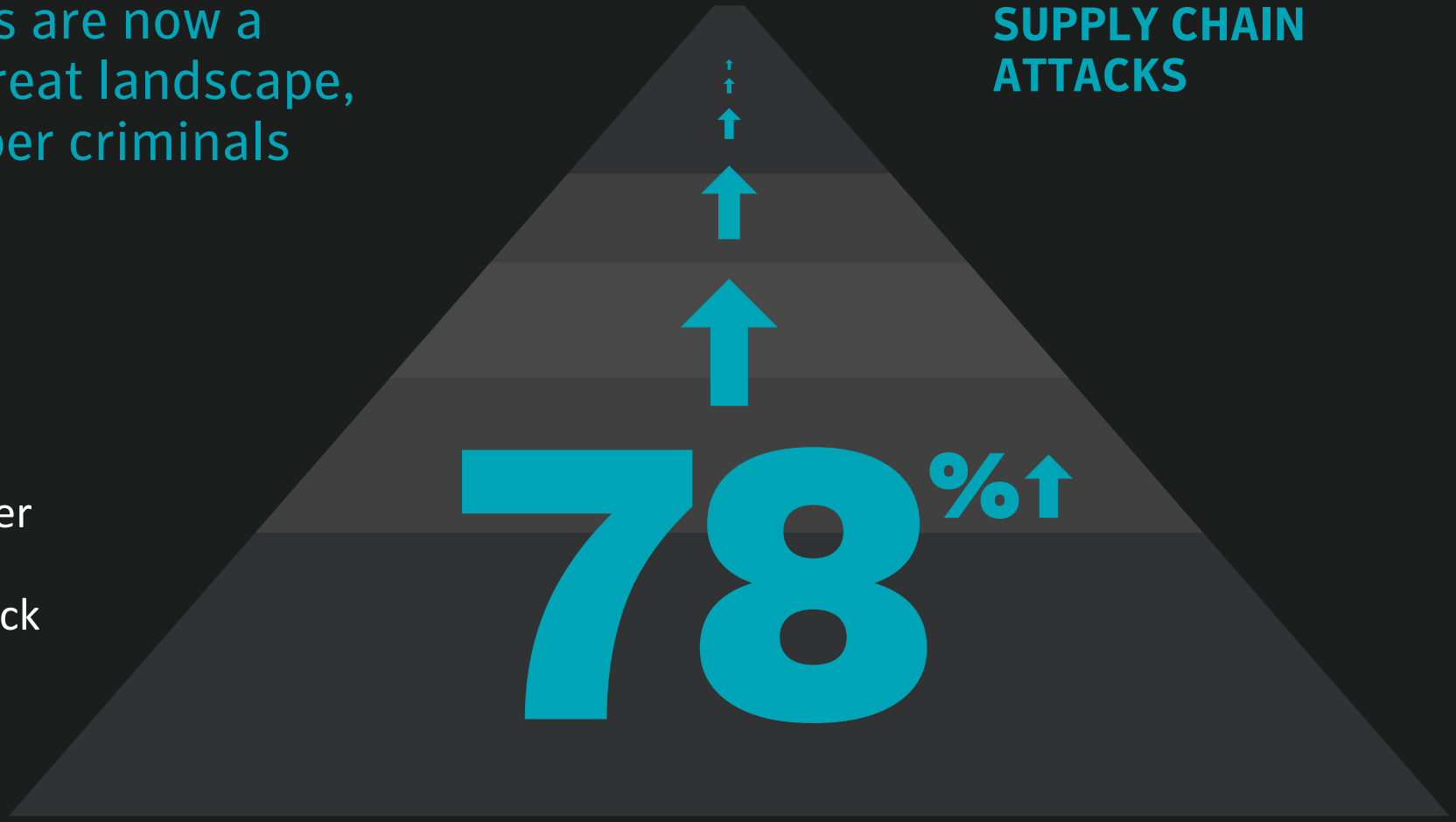


- Poorly secured cloud databases continue to be the Achilles heel for organizations
- At least 70 million records leaked from S3 buckets in 2018, many from very large companies, typically as a result of poor configuration by the owner
- Numerous widely available online tools allow potential attackers to identify misconfigured cloud resources
- Discovery of vulnerabilities in hardware chips also place cloud services at risk: Meltdown, Spectre, Foreshadow
  - An attacker who rents space on a cloud server with the Meltdown vulnerability could gain access to the protected memory spaces of other companies' resources hosted on the same physical server

Living off the Land Tools & Supply Chain Weaknesses Spur Stealthier, More Ambitious Attacks

Supply chain & LotL attacks are now a mainstay of the modern threat landscape, widely adopted by both cyber criminals and targeted attack groups

The high-profile Ticketmaster formjacking breach was the result of a supply chain attack



Targeted Attacks

GROWTH IN 2018

- More established, active groups are targeting more organizations than ever before – the number of organizations targeted per attack group increased from 42 to 55 between 2015-2018
- The number of attack groups using destructive malware grew by 25% in 2018
- Spear-phishing remains the primary vector for targeted attacks

MOTIVES

- Targets are diversifying, with a growing number of groups displaying interest in compromising operational systems, e.g. Thrip targeting operational systems that monitor and control satellites
- Intelligence gathering is still the primary motive overall

LIVING OFF THE LAND

- Zero-day vulnerabilities have become much more difficult to find, with only 23% of attack groups leveraging zero days in 2018 down from 27% in 2017– has led attackers to adopt more Living off the Land techniques

ARRESTS

- Large increase in US indictments related to state-sponsored espionage: 49 in 2018 vs. 4 in 2017

Example of timeline of notable targeted attack incidents 2016

SABOTAGE

SUBVERSION

Destructive malware used in cyberattacks against power stations in Ukraine

Buckeye begins campaign against targets in Hong Kong

Microsoft patches IE zero day which was being used in targeted attacks in South Korea

Equation Breach—exploits and malware dumped online

Disk-wiping malware Shamoon reappears after four years

JAN .... FEB .... MA .... APR .... MAY .... JUN .... JUL .... AUG .... SEP .... OCT .... NOV .... DEC

R

Seven Iranians charged in relation to cyberattacks against US targets

Data stolen from Democratic National Committee (DNC) intrusion released online

Symantec uncovers Strider cyberespionage group

WADA

Data stolen from World Anti-Doping Agency (WADA) intrusion released

Power outages in Ukraine suspected to be linked to cyberattack

Resurgence of sabotage

Sabotage campaigns represent another form of politicized and disruptive attack

Shamoon *est. 2012*

Aliases / Distrack

Tools, tactics & procedures (TTP)

- Stage one: Spear-phishing, credential theft
- Stage two: Disk-wiping payload

Motives

- Aggressive and highly disruptive campaigns
- Political: payload includes political imagery

Target categories & regions

- Energy
- Saudi Arabia

Known for

- 2012 campaign against Saudi and Qatari energy sector
- Reappearance with broader campaign in 2016

Sandworm *est. 2014*

Aliases / Quedagh, BE2 APT

Tools, tactics & procedures (TTP)

- Killdisk disk-wiping threat
- Stealth: deletes logs, removes attack artifacts
- Maximum disruption: blocks access to recovery systems

Motives

- Political, military: cyber wing of ongoing against Ukraine

Target categories & regions

- Critical infrastructure, energy, media, finance
- Ukraine

Known for

- Late 2015 power outage in Ukraine
- War-dialing of energy companies

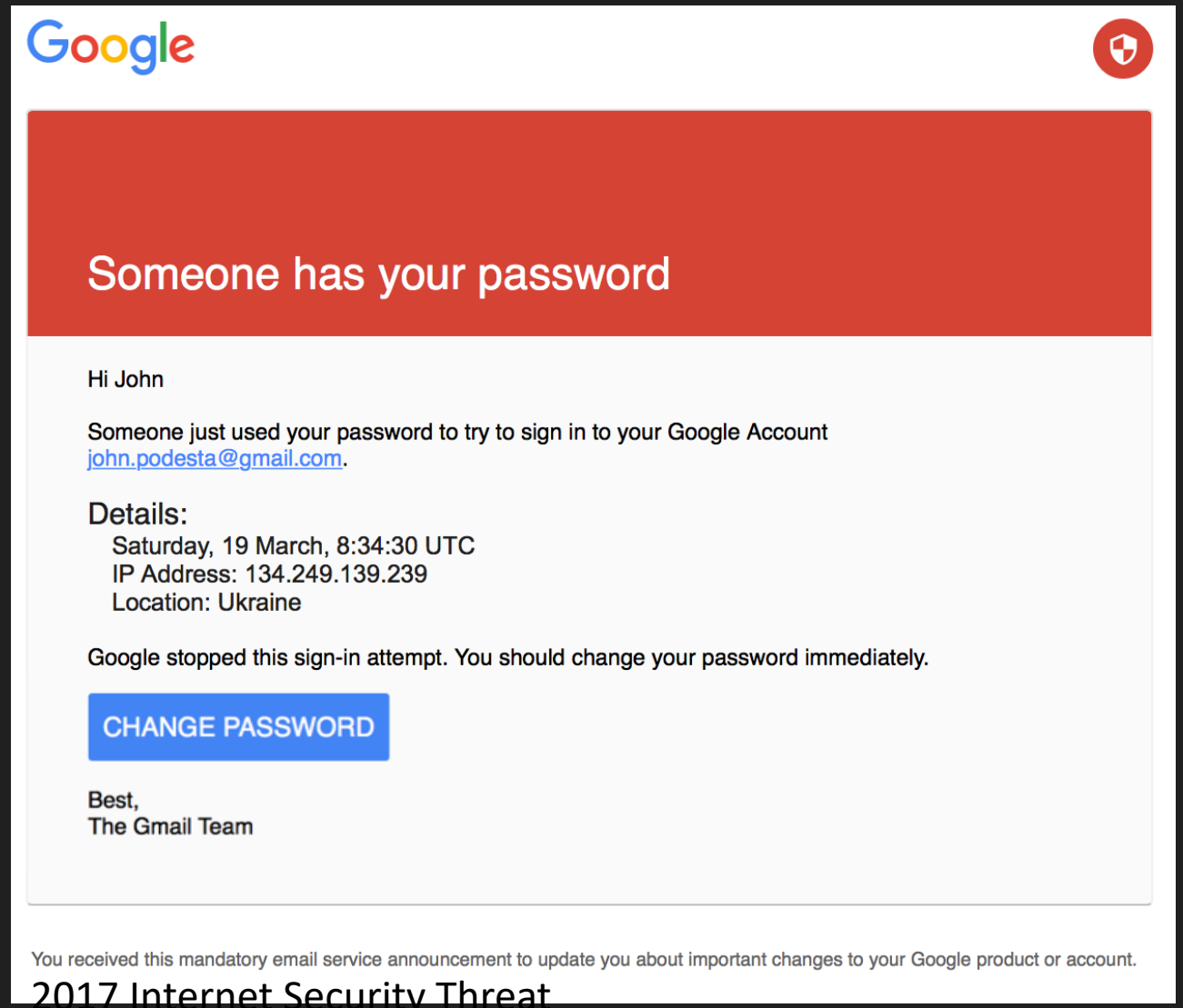
John Podesta

From Wikipedia, the free encyclopedia

John David Podesta (born January 8, 1949) is a columnist and former chairman of the 2016 Hillary Clinton presidential campaign.[1] He previously served as chief of staff to President Bill Clinton and Counselor to President Barack Obama.[2]

He is the former president, and now Chair and Counselor, of the Center for American Progress (CAP), a liberal think tank in Washington, D.C., as well as a Visiting Professor of Law at the Georgetown University Law Center. Additionally, he was a co-chairman of the Obama-Biden Transition Project.[3][4]

Anatomy of a Targeted Phishing Attack



Google

Someone has your password

Hi John

Someone just used your password to try to sign in to your Google Account john.podesta@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD

Best,
The Gmail Team

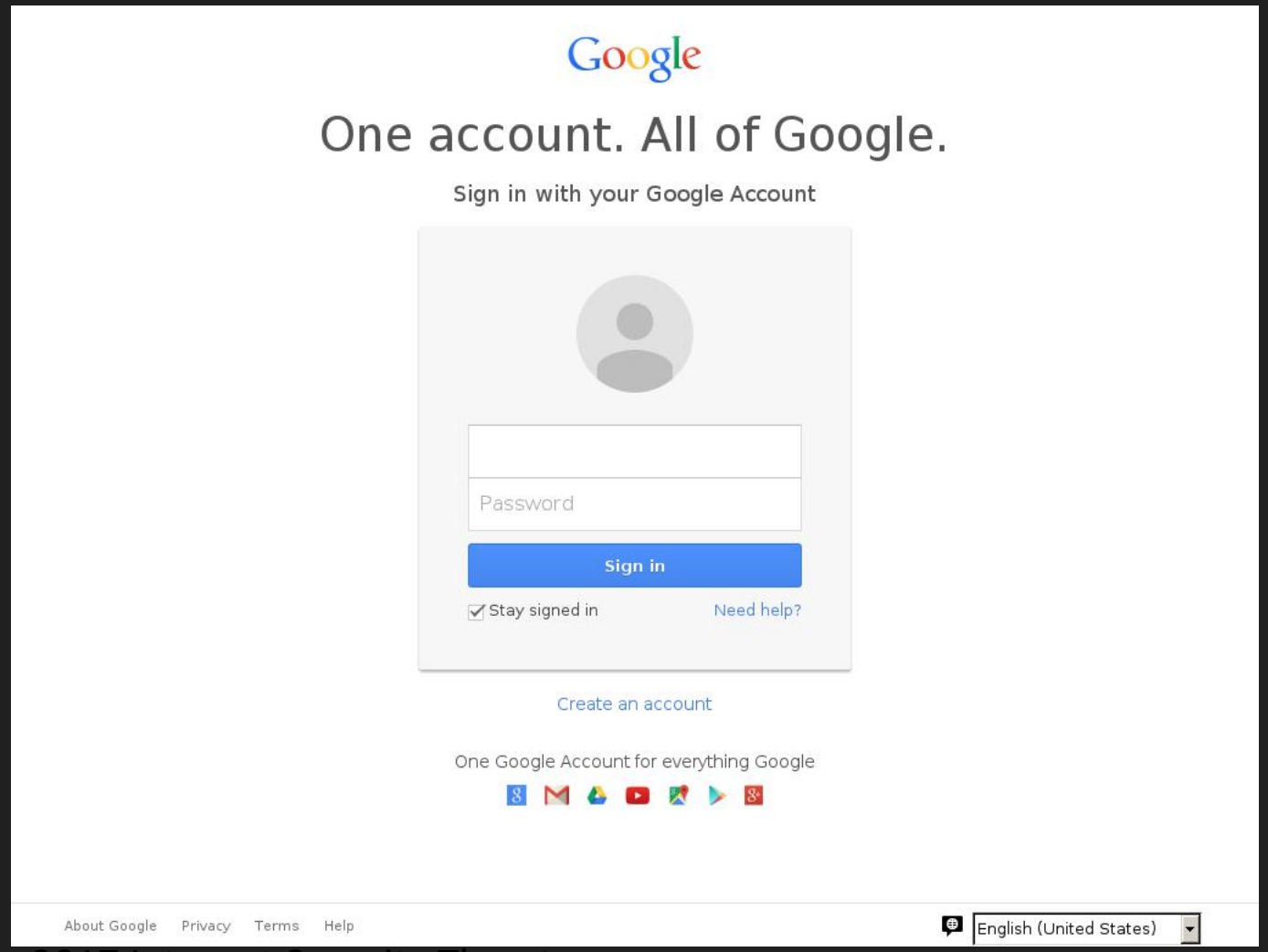
You received this mandatory email service announcement to update you about important changes to your Google product or account.

- The branding looks consistent (Google logo, shield logo)
- The email is addressed to the recipient (not “Dear Sir”)
- The English is not broken

2017 Internet Security Threat Report | Volume 22

Anatomy of a Targeted Phishing Attack

Anatomy of a Targeted Phishing Attack



- The login page looks identical to the actual login page (HTML was cloned)
- Once the user submits the username/password combination, it doesn't matter what happens next
  - Typically, the phishing page redirects users back to Google.com

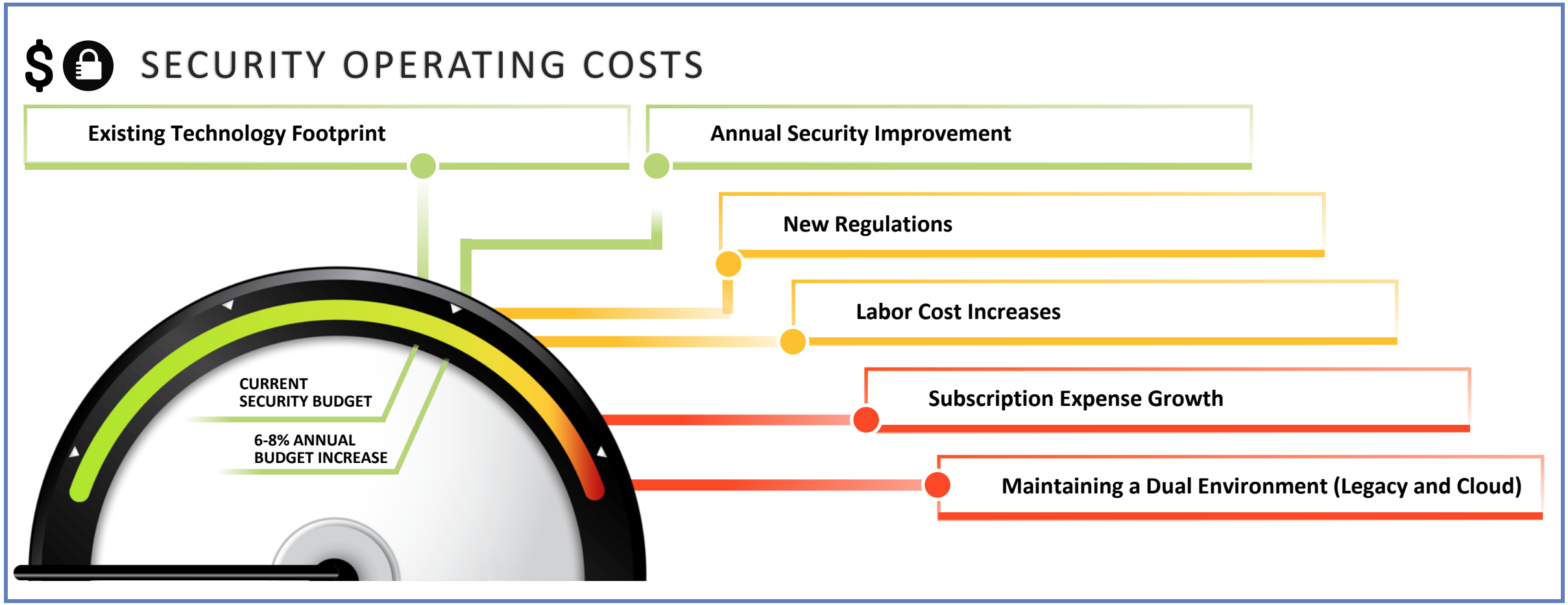
This is a legitimate email. John needs to change his password immediately, and ensure that two-factor authentication is turned on his account.

He can go to this link: https://myaccount.google.com/security to do both. It is absolutely imperative that this be done ASAP.

Where is technology going?
What are the policy implications?

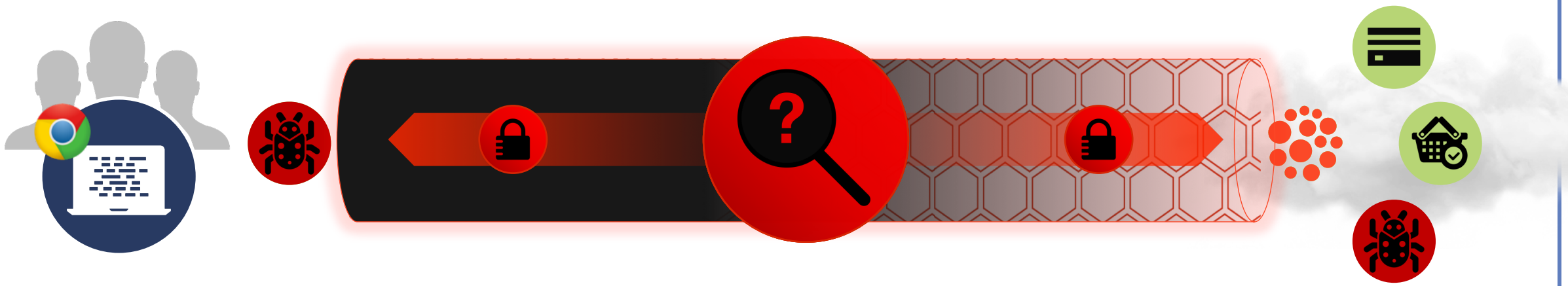
Cost of technology, compliance and skill

The Industry Faces a Looming Fiscal Spending Crisis



The “going dark” of the internet

A Dark Internet Will Require Presence at Key Termination Points

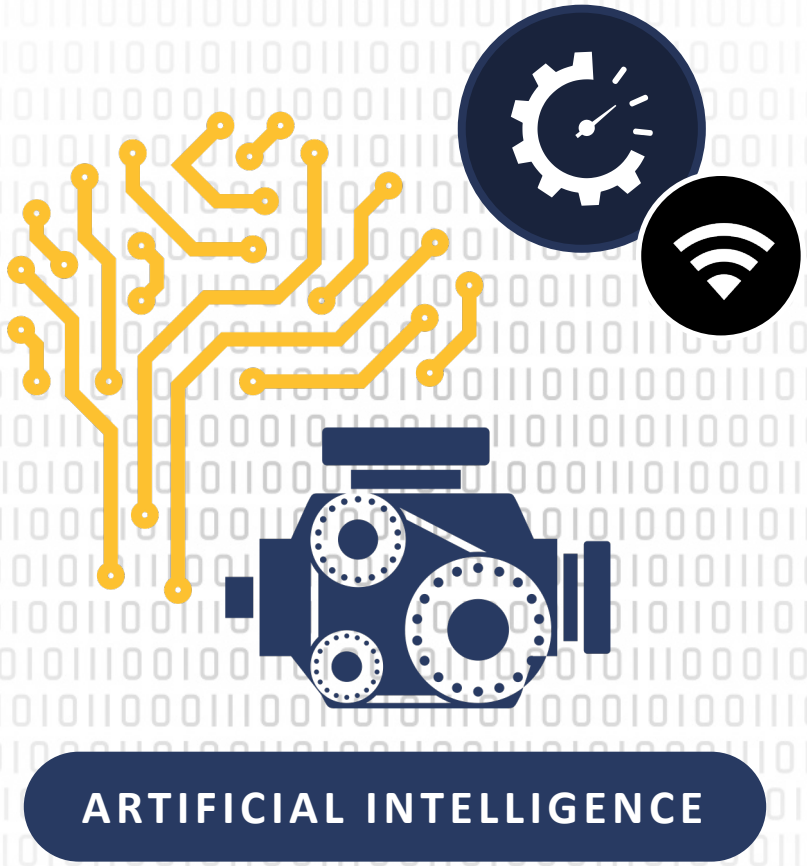


IoT security can be as chaotic

IT		IoT
"Open" Easy to install	*Openness*	**"Closed"** Not open to new software after device leaves factory
"3" (Mostly UDP, TCP, IP)	*Protocols*	**Thousands of Protocols** (Hundreds in each vertical)
"5" (Mostly Windows, Linux, OSX, iOS, Android)	*Operating Systems (OS)*	**Dozens** (Heavily fragmented by vertical)
20k seat enterprise (Typical Enterprise)	*Scale*	**100M "things"** (Typical Car Maker)
All verticals have **same** Hardware/OS supply chain	*Fragmentation*	Each verticals has **different** Hardware/OS supply chain
"2" X86 and x64 by Intel and AMD	*Chipset Architectures*	**Many** 8bit AVR,16bit MCU,32/64bit ARM,x86/64;12+vendors

The use of AI and cyber

Organizations Will Need to Depend on Automatic Security Capabilities



Attacking AI is more than just hacking

Issues to consider

- Cyber as a distinct defense and international politics discussion is here to stay
- All defense projects will increasingly have a heavier focus on cybersecurity
- No single magical solution
- Trust issues will continue
- Militarization of some technologies is inevitable
- Cybersecurity moving towards SIGINT, EW, sabotage and strategic warfare
- Cloud computing, mobility, AI, IoT, smart grid and big data, new solutions and challenges

QUESTIONS