AGH
CPAs & ADVISORS

Cybersecurity: Protect Your Organization from Cybercriminals

October 24, 2017

The webinar will start at noon CT

Brian Johnson, CISA, CISM, CGEIT, CRISC
Senior Vice President, Technology Services

Administration

SHRM
SHRM-CP | SHRM-SCP
RECERTIFICATION
PROVIDER
2017

NATIONAL REGISTRY OF
CPE
SPONSORS

If you need HR or CPE credit, please participate in all polls throughout the presentation.

Administration

A recording of today’s webinar will be emailed for your reference or to share with others.

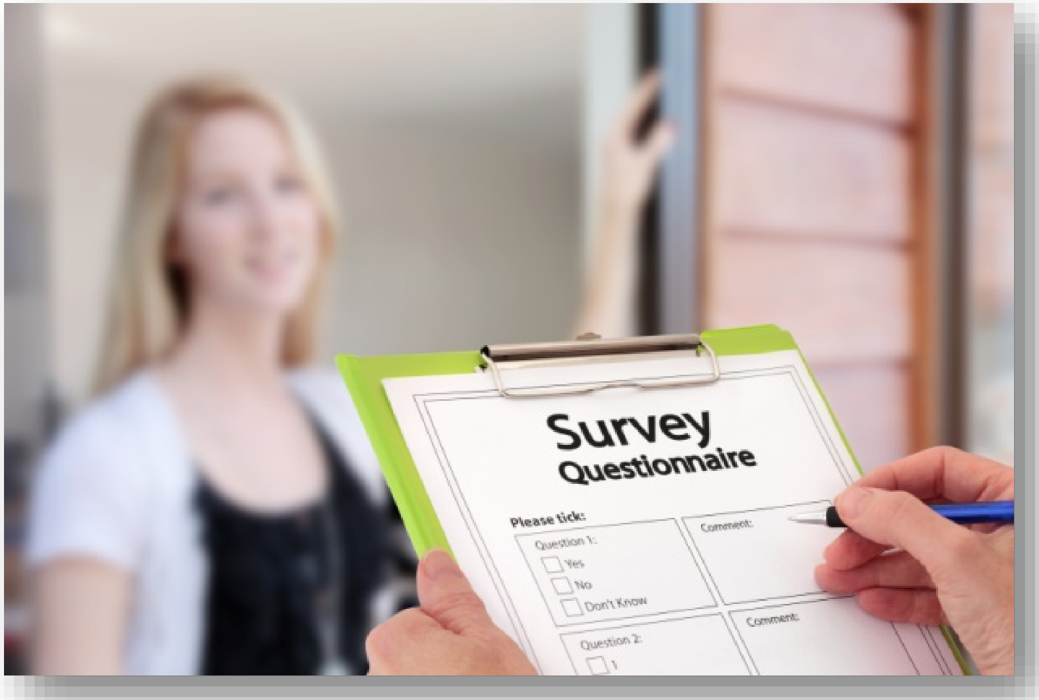
Administration

For best quality, call in by phone instead of using your computer speakers.

Administration

To ask questions during the presentation, use the questions box on the right side of your screen.

Administration



Please provide your feedback at the end of today's presentation.

About the Speaker

Brian Johnson, CISA, CISM, CGEIT, CRISC
Senior Vice President,
Technology Services

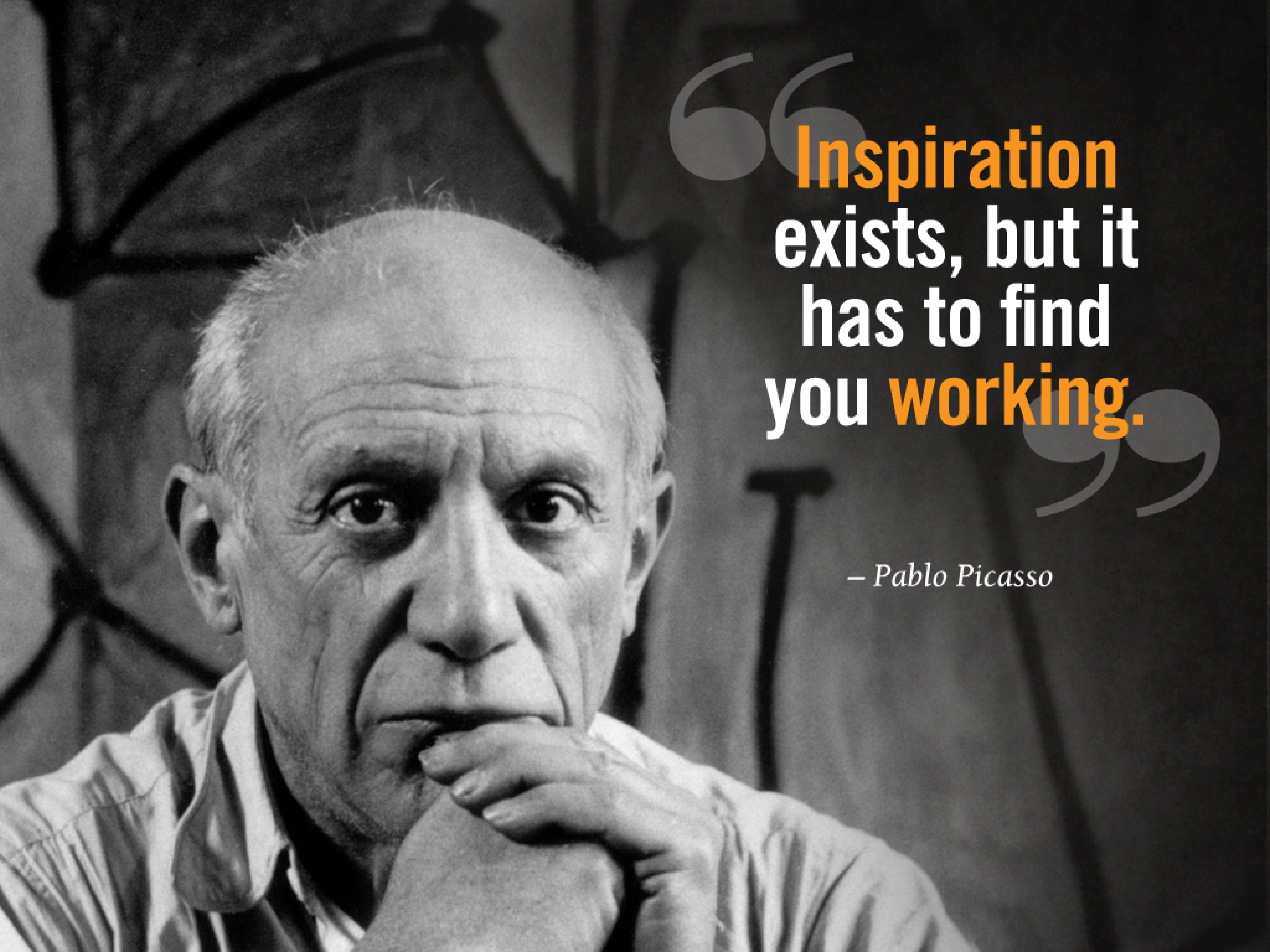
30 years' experience leading technology initiatives for business solutions; certified public accountant

Extensive credentials in IT security, risk management, and enterprise technology governance, in addition to specialized systems and application credentials

AGH
CPAs & ADVISORS

Cybersecurity

Will you be prepared for the future?



“Inspiration exists, but it has to find you working.”

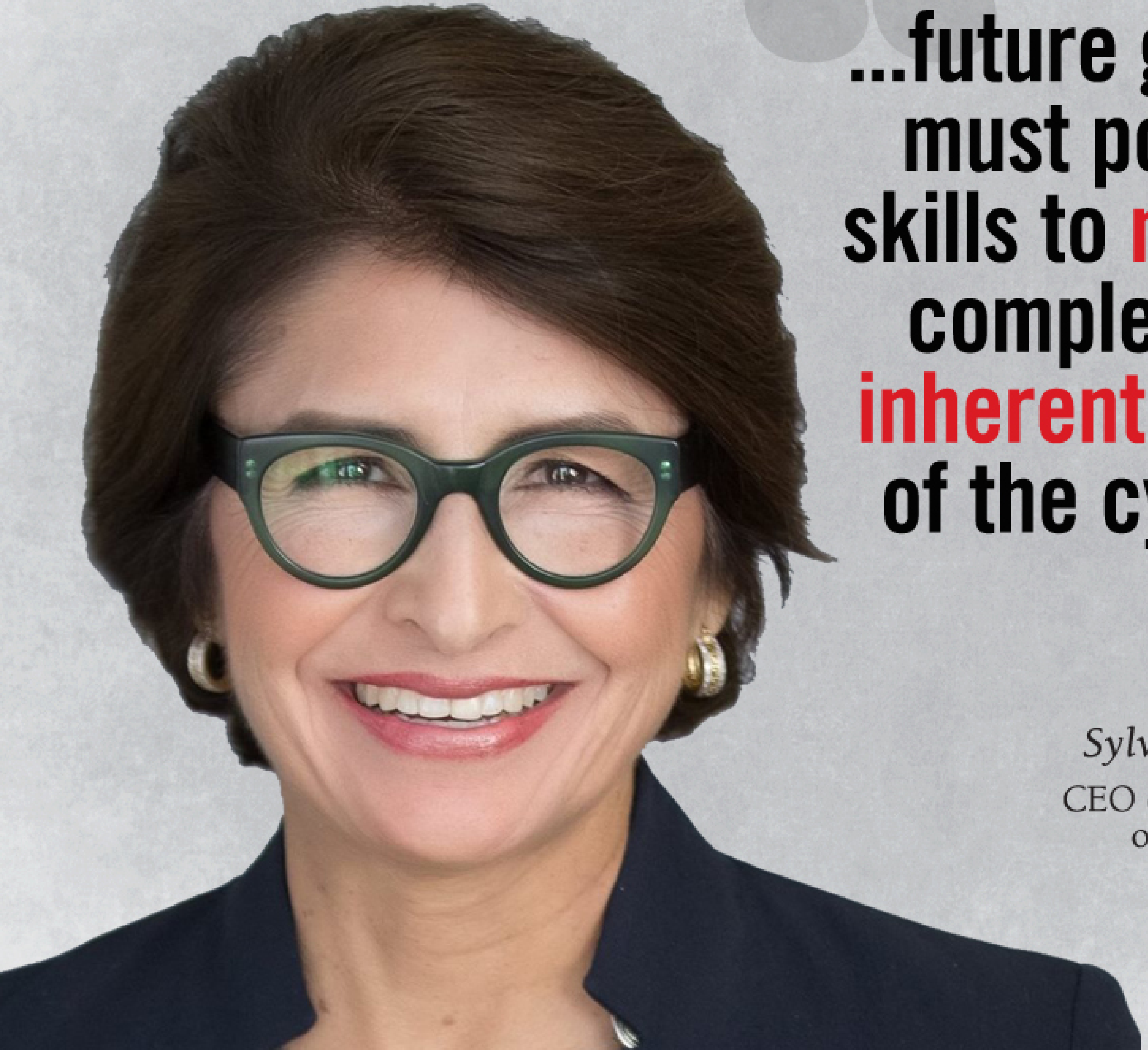
– Pablo Picasso

Today’s Girl Scouts will be...

The Girl Scouts & Palo Alto Networks are **preparing girls** for the future of **cybersecurity.**

September 2018

18 Cybersecurity badges for girls K-12



> ...future generations must possess the skills to navigate the complexities and inherent challenges of the cyber realm.

Sylvia Acevedo

CEO of Girl Scouts
of the USA

Daisies (Grades K-1) & Brownies (Grades 2-3)

Will learn where information goes, and how a computer works.

Juniors (Grades 4-5) &
Cadettes (Grades 6-8)

Will learn how viruses work,
and how cyberattacks happen.

Seniors (Grades 9-10) & Ambassadors (Grades 11-12)

Will study social engineering, and how psychological manipulation of people works in phishing attempts.

Young girls wanted to know how to make sure they don’t get bullied online...

Older girls wanted to know how to prevent cyberattacks.

Sylvia Acevedo

CEO of Girl Scouts
of the USA

Females represent only 11% of the cybersecurity workforce.

Source: Center for Cyber Safety and Education & $(ISC)^2$

Adjust your perspective.

Message Objective

By better understanding some of the most dangerous and prevalent cyberthreats, you can learn how to combat the increasing volume and sophistication of cyberattacks and defend your business from cybercriminals.

AGENDA:

1. Why does this matter?
2. Where are the imminent threats?
3. What is Management's role?

AGENDA:

1. Why does this matter?
2. Where are the imminent threats?
3. What is Management's role?

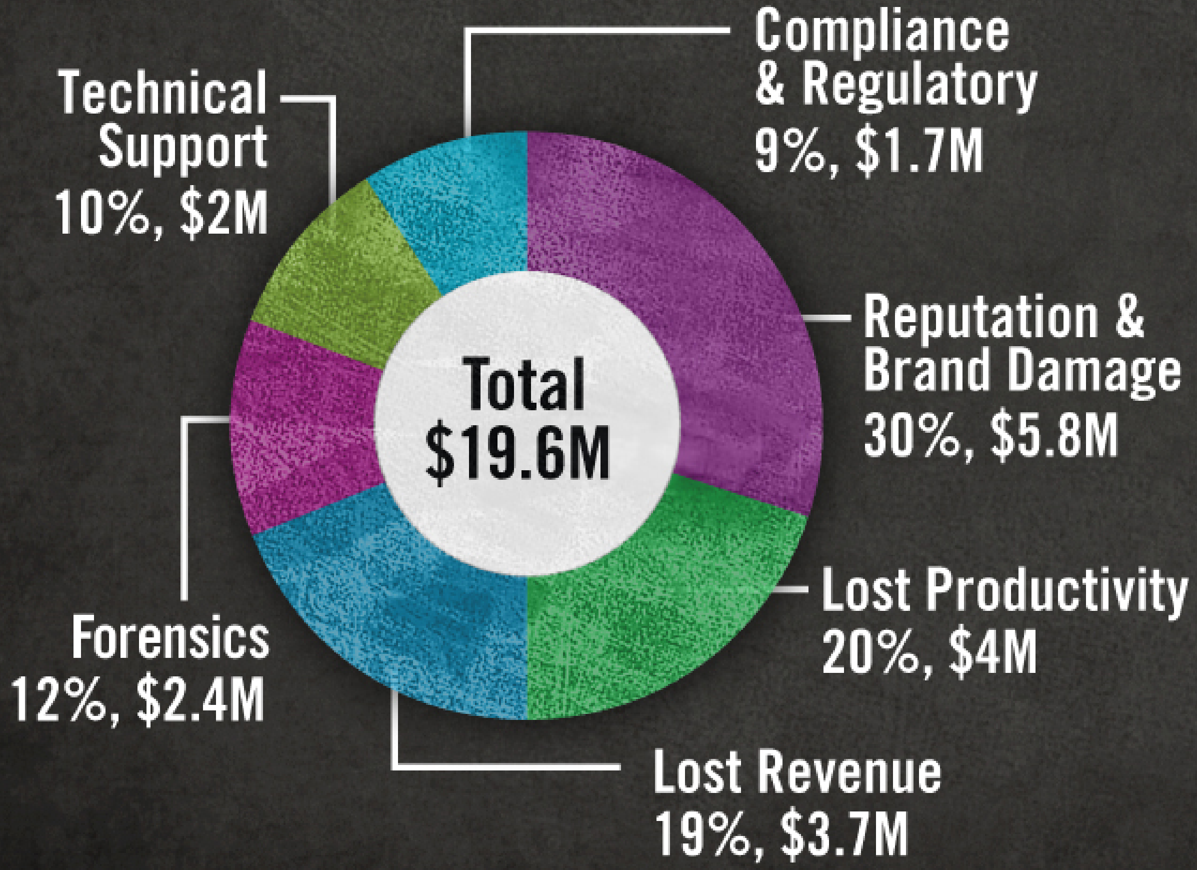
Why does this matter to me?

$3.06 TRILLION

Total
global impact
of cybercrime.

Source: Increased Cyber Security Can Save Global Economy Trillions, McKinsey World Economic Forum

Financial Impact by Cost Category



Business costs make up more than

75%

of the financial consequences of business continuity and IT security failures.

Source: Implications of the IBM Global Study on the Economic Impact of IT Risk

Think differently.

Polling Question #1

AGENDA:

1. Why does this matter?
2. Where are the imminent threats?
3. What is Management’s role?

Where are the **imminent threats** to my business?

Imminent Threats

- Ransomware
- Social Engineering
- Internet of Things

Ransomware:

A type of malicious attack where the attackers encrypt the organization's critical data, such as personal data or business data, after they have infiltrated the systems, then demand a monetary payment in digital cash formats, such as bitcoin.

Source: NIST Special Publication 800-184

Ransomware is growing at a yearly rate of 350%

Source: Cisco – 2017 Annual Cybersecurity Report

In 2016, **40%** of spam emails contained links to ransomware, an increase of **6000%** over 2015, when less than **1%** contained such links.

Source: IBM Security – Ransomware: How Consumers and Businesses Value Their Data

Global ransomware damage costs predicted to exceed

$5 billion

in 2017, up from

$325 million

in 2015

Source: Cybersecurity Ventures – 2017 Ransomware Damage Report

70% of business ransomware targets paid the ransom

- Half of those paid over $10,000
- 20% paid over $40,000

Source: IBM Security – Ransomware: How Consumers and Businesses Value Their Data

ASK

Staff Training:

Have we trained staff on cybersecurity best practices?

Source: U.S Interagency Report – Ransomware: What It Is and What To Do About It

ASK

Backups:

Do we backup all critical information?

Are the backups stored offline?

Have we tested our ability to revert to backups during an incident?

Incident Response:

ASK

Do we have an incident response plan and have we exercised it?

Source: U.S Interagency Report – Ransomware: What It Is and What To Do About It

Business Continuity:

ASK

Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?

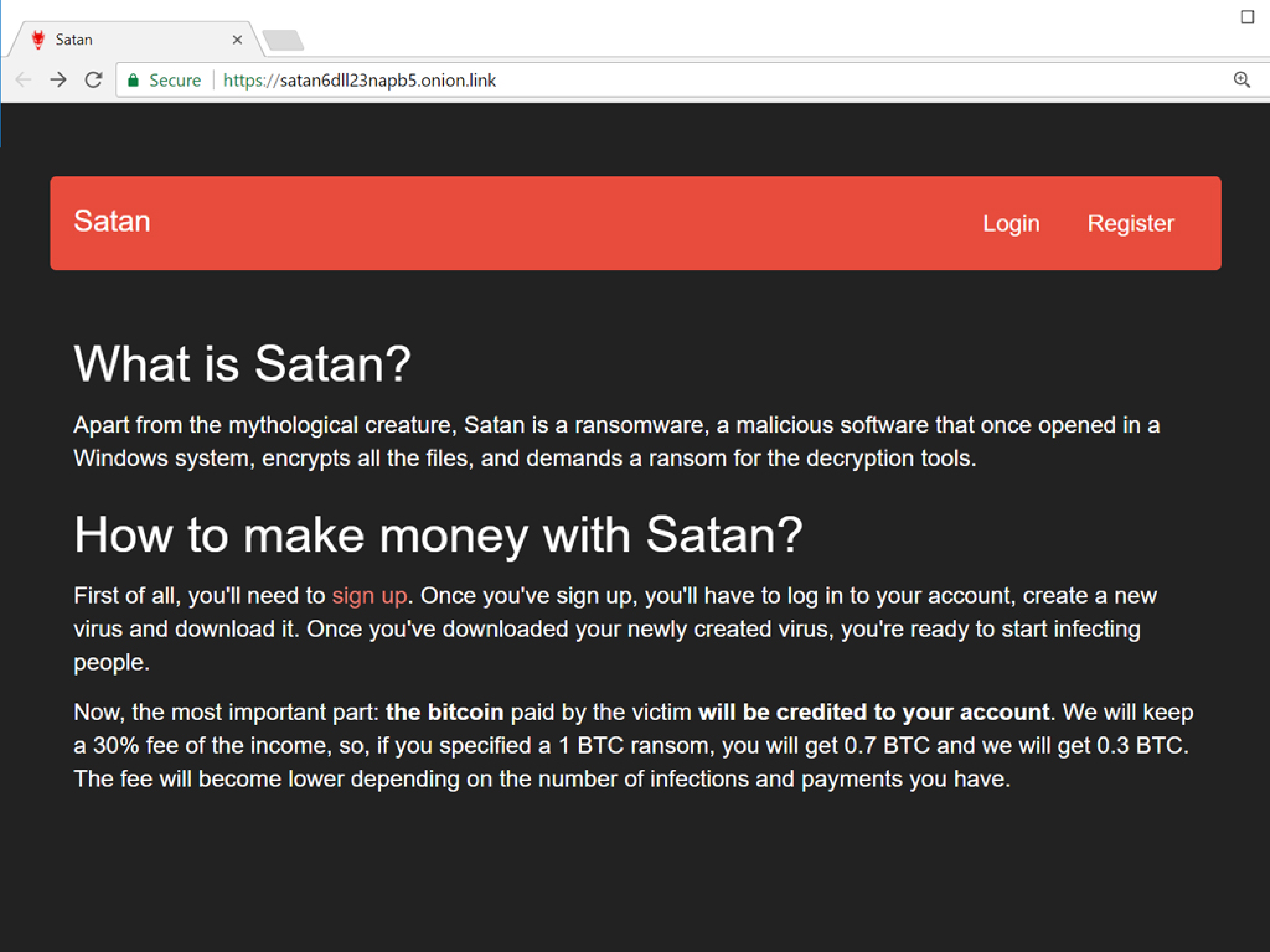
Source: U.S Interagency Report – Ransomware: What It Is and What To Do About It

Vulnerability Patching:

ASK

Have we implemented appropriate patching of known system vulnerabilities?

Source: U.S Interagency Report – Ransomware: What It Is and What To Do About It



Satan

Login Register

What is Satan?

Apart from the mythological creature, Satan is a ransomware, a malicious software that once opened in a Windows system, encrypts all the files, and demands a ransom for the decryption tools.

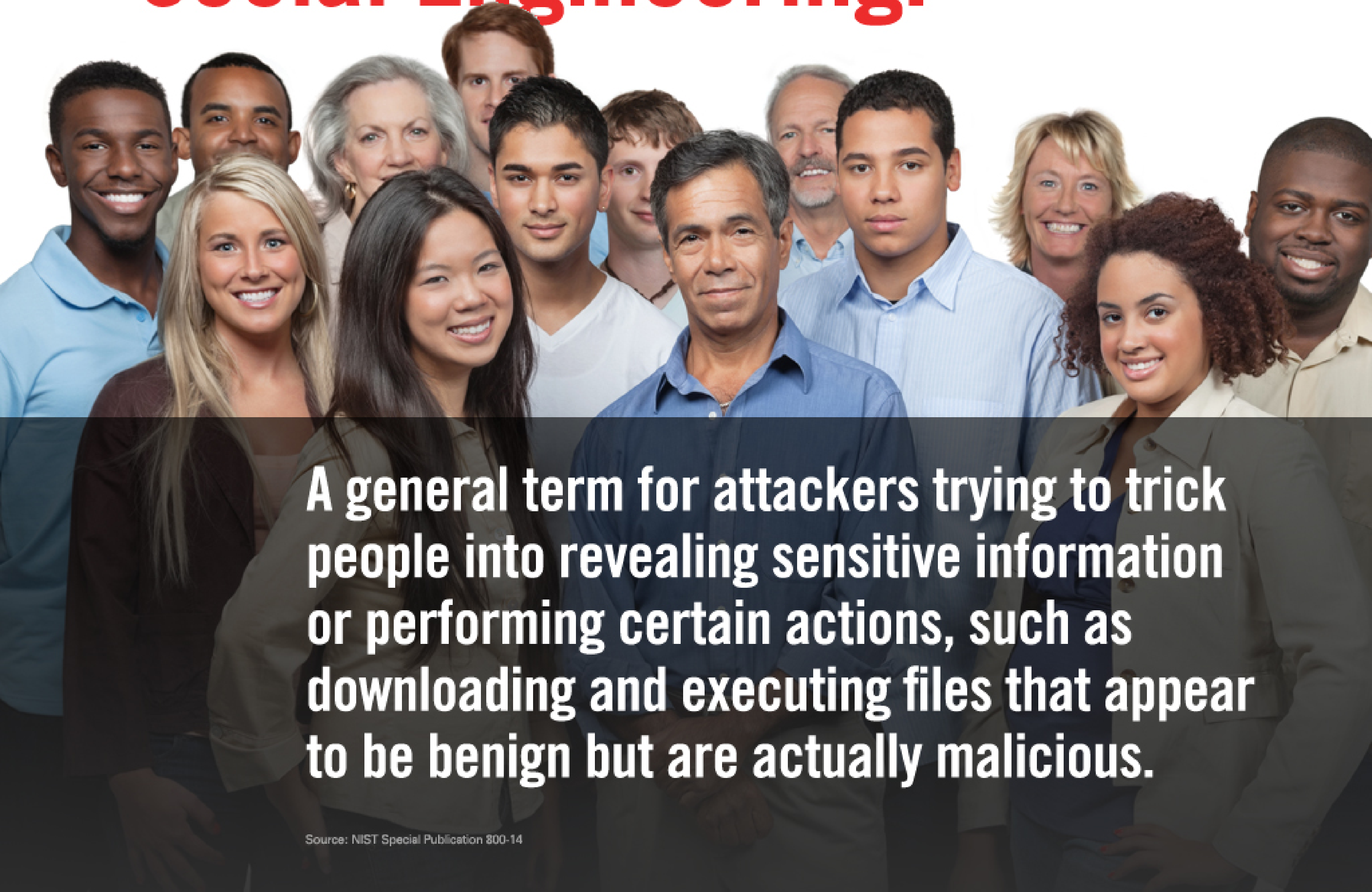
How to make money with Satan?

First of all, you'll need to sign up. Once you've sign up, you'll have to log in to your account, create a new virus and download it. Once you've downloaded your newly created virus, you're ready to start infecting people.

Now, the most important part: **the bitcoin** paid by the victim **will be credited to your account**. We will keep a 30% fee of the income, so, if you specified a 1 BTC ransom, you will get 0.7 BTC and we will get 0.3 BTC. The fee will become lower depending on the number of infections and payments you have.

Polling Question #2

Social Engineering:



A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.

Source: NIST Special Publication 800-14

Phishing:

A digital form of social engineering that tries to obtain financial or other confidential information from Internet users, typically by sending an email that looks as if it is from a legitimate organization, encouraging an end user to take an action that compromises their computer or reveals sensitive information.

Source: Wombat Security State of the Phish 2017

More than **400 businesses** are targeted by Business Email Compromise (BEC) scams every day.

Source: Symantec 2017 Internet Security Threat Report (ISTR)

BEC scams have accounted for more than **$5 billion in losses** between October 2013 and December 2016, with more than 24,000 victims reporting incidents worldwide.

Source: FBI Internet Crime Complaint Center (IC3) - Alert Number I-050417-PSA

Reports of W-2 phishing emails increased **870%** in 2017.

> "The criminals are especially brazen. In one case, a criminal did not like the format the W-2s were in, so the thief asked the payroll employee to reformat and resend them. The employee complied."

Source: IRS Return Integrity Compliance Services

Source: Tamara Powell, acting director of the IRS Return Integrity Compliance Services

ASK

Staff Training:

Have we trained staff to recognize social engineering and phishing attack methods? Do we test their understanding with simulated attacks?

Source: US-CERT Security Tip (ST04-014) Avoid Social Engineering and Phishing Attacks

Email:

Do we reveal personal or financial information in email? Do we respond to email solicitations for this information, which includes following links sent in email?

Source: US-CERT Security Tip (ST04-014) Avoid Social Engineering and Phishing Attacks

ASK

Websites:

Do we send sensitive information over the Internet before checking a website's security?

vSource: US-CERT Security Tip (ST04-014) Avoid Social Engineering and Phishing Attacks

URLs:

ASK

Do we pay attention to the URLs of a website? Do we understand that malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain?

Source: US-CERT Security Tip (ST04-014) Avoid Social Engineering and Phishing Attacks

ASK

Protection:

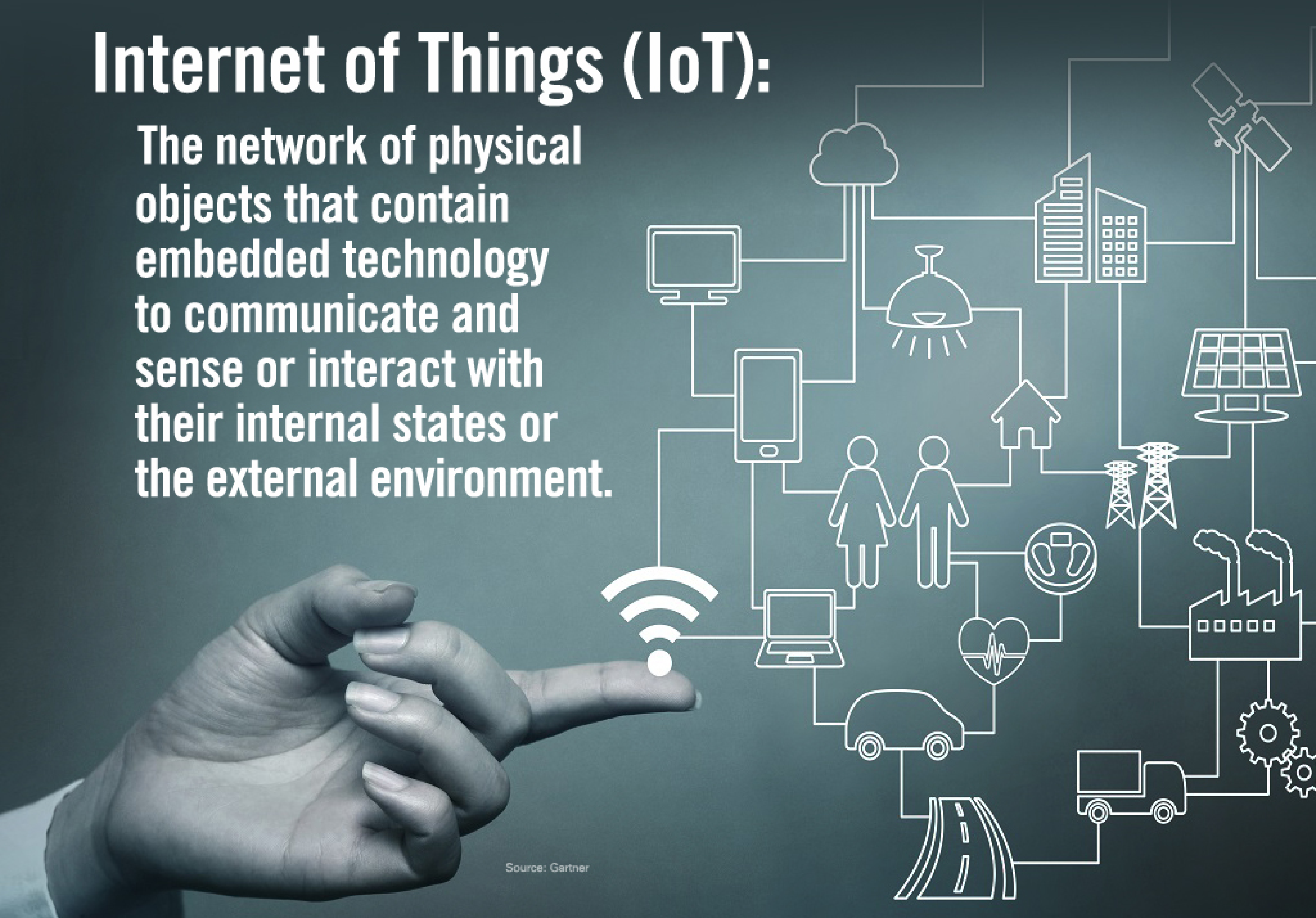
Have we installed and maintained anti-virus software, firewalls, and email filters to reduce some of this traffic? Do we take advantage of any anti-phishing features offered by our email client and web browser?

Source: US-CERT Security Tip (ST04-014) Avoid Social Engineering and Phishing Attacks

Polling Question #3

Internet of Things (IoT):

The network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.



Source: Gartner

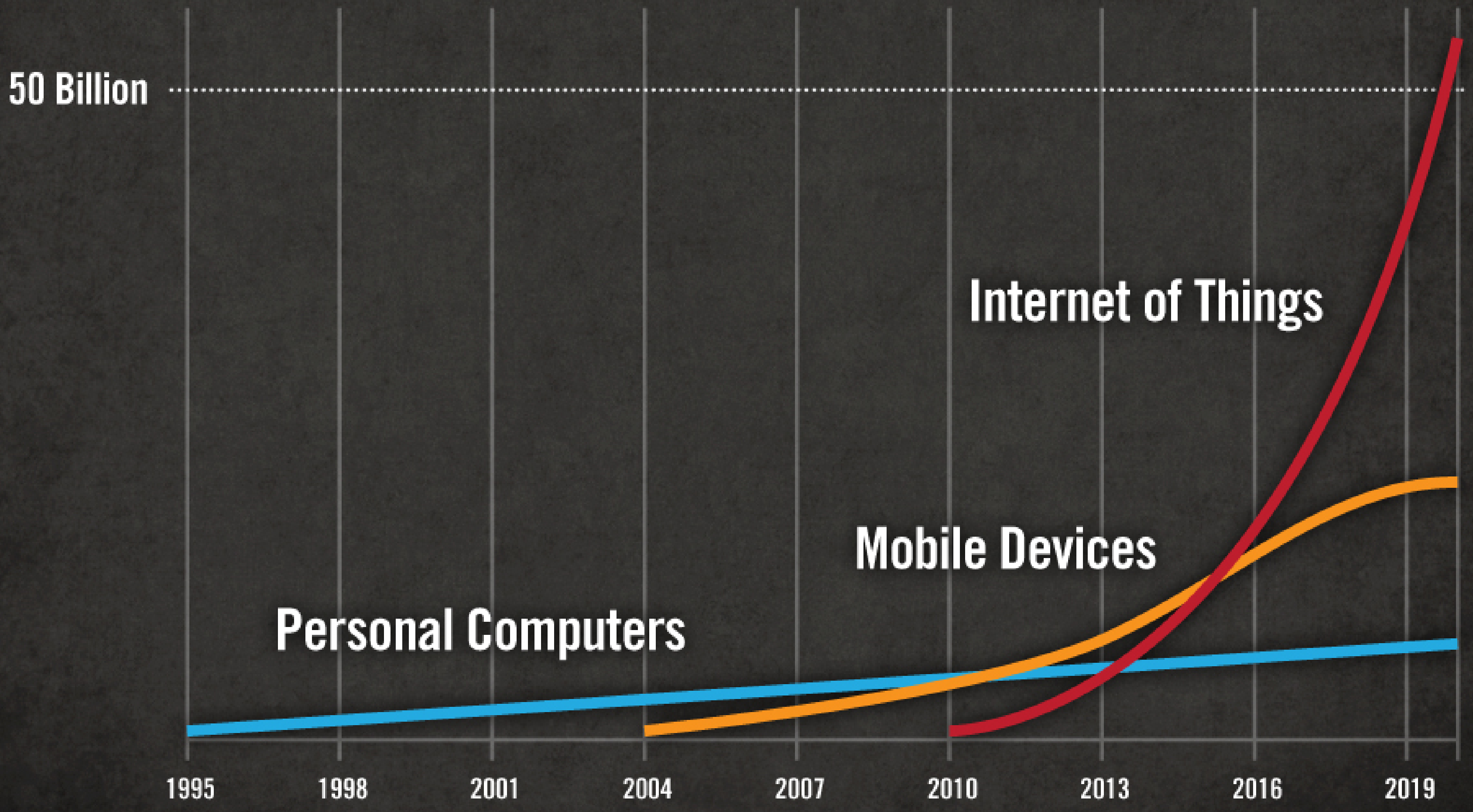
The Internet of Things

World Population	6.3 Billion	6.8 Billion	7.2 Billion	7.6 Billion
Connected Devices	500 Million	12.5 Billion	25 Billion	50 Billion
Devices Per Person	0.08	1.84	3.47	6.58
	2003	2010	2015	2020

MORE CONNECTED DEVICES THAN PEOPLE

Source: Cisco IBSG, April 2011

Global Internet Connected Devices



Sources: McAfee, based on research by BI Intelligence, IDC, and Intel.

Medical Devices
Hard-Coded Passwords

ICS-CERT reported that around 300 machines from 40 vendors have hard-coded passwords. The affected devices are manufactured by a broad range of vendors and fall into a broad range of categories including but not limited to:

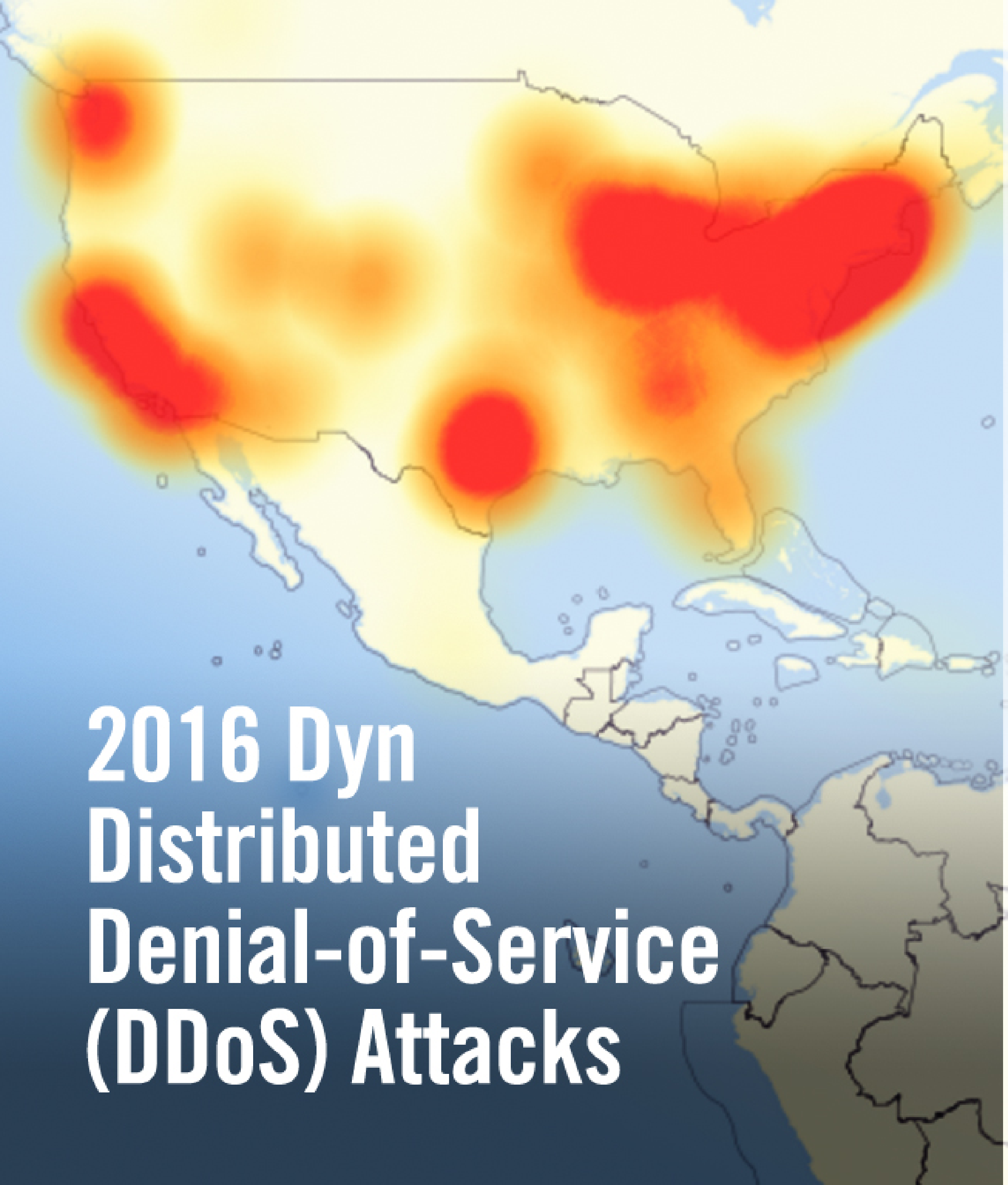
- Pacemakers
- Drug infusion pumps
- Surgical and anesthesia devices
- Ventilators
- External defibrillators
- Patient monitors
- Laboratory and analysis equipment

Sources: ICS-CERT Alert (ICS-ALERT-13-164-01) Medical Devices Hard-Coded Passwords; Advisory (ICSMA-17-241-01) Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities; and ICS-CERT Advisory (ICSMA-17-250-02) Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump Vulnerabilities

Fiat Chrysler recalled 1.4 million vehicles after researchers demonstrated a proof-of-concept attack where they managed to take control of the vehicle remotely.

In the UK, thieves hacked keyless entry systems to steal cars.

Source: Symantec 2016 Internet Security Threat Report (ISTR)



2016 Dyn Distributed Denial-of-Service (DDoS) Attacks

The attacks were executed through a botnet attack consisting of large numbers of Internet-connected devices that had been infected with the Mirai malware.

ASK

Purpose:

Do we fully understand the capabilities and associated risks of our IoT devices? Are our IoT devices the ideal solution for their intended purposes?

Source: Source: FBI Internet Crime Complaint Center (IC3) - Alert Number I-091015-PSA

Network Security:

ASK

Do we isolate our IoT devices on their own network? Do we allow devices to remotely connect and communicate with the IoT devices on our network automatically without authentication? Do our IoT devices allow open Wi-Fi connections?

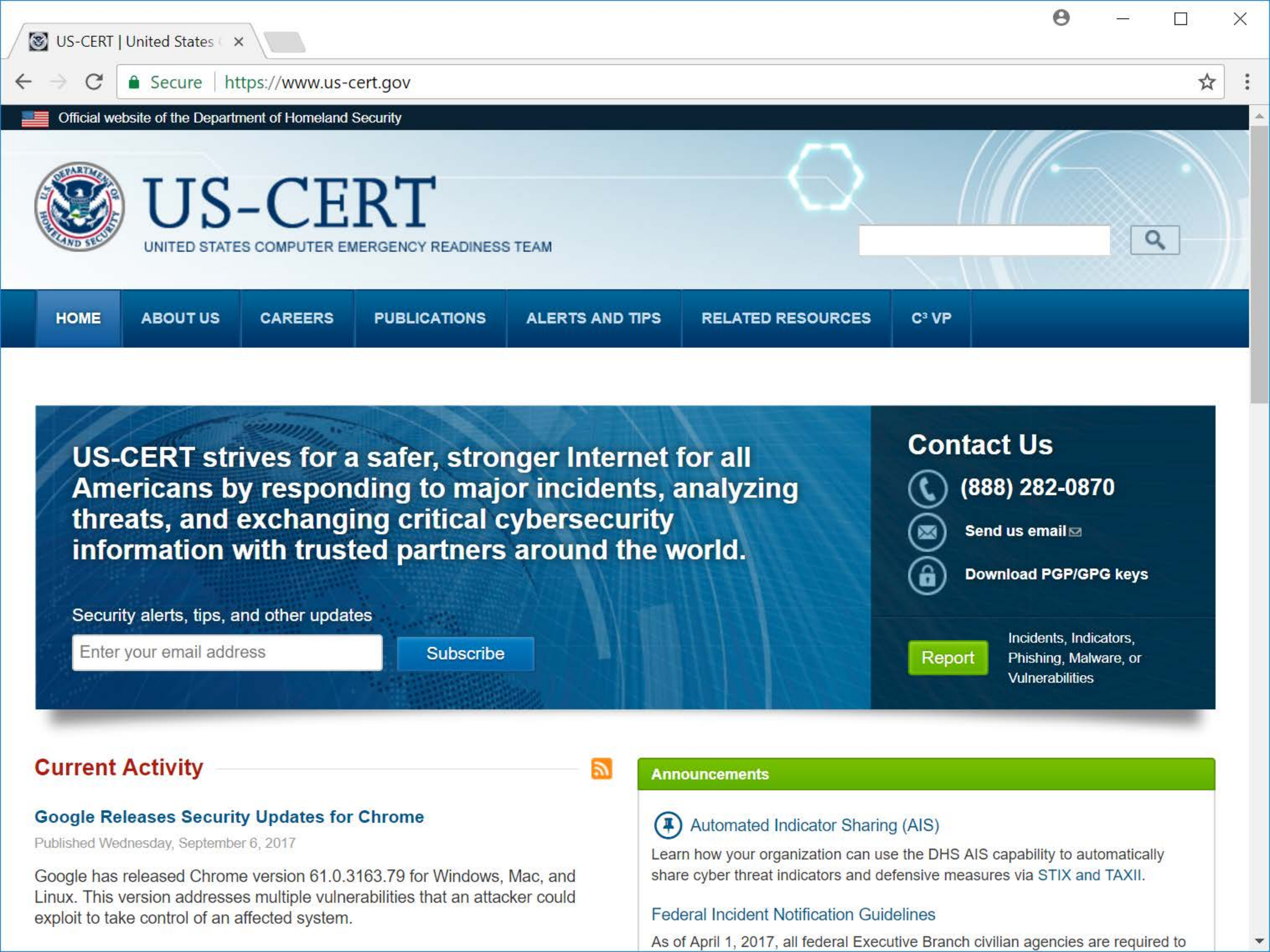
Source: Source: FBI Internet Crime Complaint Center (IC3) - Alert Number I-091015-PSA

Device Security

ASK

Do we purchase our IoT devices from manufacturers with a proven track record of providing secure devices? Do we update our IoT devices with security patches? Do we change the default passwords on our IoT devices and use strong passwords?

Source: Source: FBI Internet Crime Complaint Center (IC3) - Alert Number I-091015-PSA



Official website of the Department of Homeland Security

US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.

Security alerts, tips, and other updates

Contact Us

☎ (888) 282-0870

Send us email

Download PGP/GPG keys

Incidents, Indicators, Phishing, Malware, or Vulnerabilities

Current Activity

Google Releases Security Updates for Chrome

Published Wednesday, September 6, 2017

Google has released Chrome version 61.0.3163.79 for Windows, Mac, and Linux. This version addresses multiple vulnerabilities that an attacker could exploit to take control of an affected system.

Announcements

Automated Indicator Sharing (AIS)

Learn how your organization can use the DHS AIS capability to automatically share cyber threat indicators and defensive measures via STIX and TAXII.

Federal Incident Notification Guidelines

As of April 1, 2017, all federal Executive Branch civilian agencies are required to

Polling Question #4

AGENDA:

1. Why does this matter?
2. Where are the imminent threats?
3. What is Management's role?

What is **Management's role** in ensuring cybersecurity?

COBIT® 5

What's in Your Survival Kit?

- Risk Identifiers
- Important Questions
- Recommended Actions

Pro

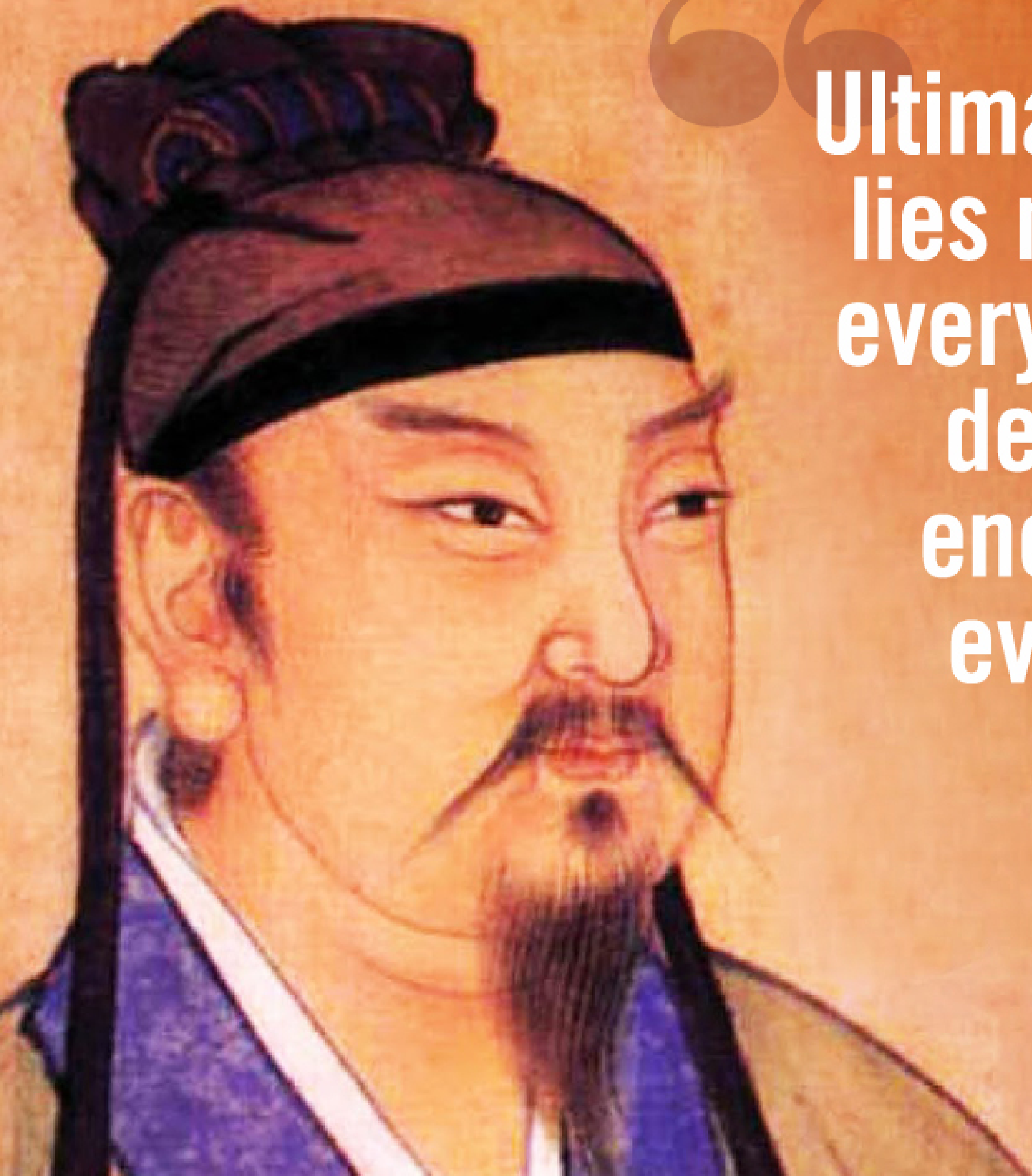
~~Re~~active

AGENDA:

1. Why does this matter?
2. Where are the imminent threats?
3. What is Management's role?

Message Objective

By better understanding some of the most dangerous and prevalent cyberthreats, you can learn how to combat the increasing volume and sophistication of cyberattacks and defend your business from cybercriminals.



“Ultimate excellence lies not in winning every battle, but in defeating the enemy without ever fighting.”

– Sun Tzu

Questions?

Brian.Johnson@aghlc.com