# IT'S TIME FOR A CYBER MOONSHOT

accenture

Observations from the 2nd Annual Cambridge Cyber Summit

By Gus Hunt, Federal Cybersecurity Practice Lead

## HERE'S A **CYBERSECURITY POP QUIZ** FOR YOU.

**The state of cybersecurity is...**

A. A frog in boiling water
B. A failure of imagination
C. A $6 trillion global criminal enterprise by the year 2021 [1]
D. All of the above

## I'M GOING TO ASSUME YOU ANSWERED D,

**and you're correct.** That's how several U.S. officials described our state of cyber affairs at the Second Annual Cambridge Cyber Summit.

Government officials and private industry leaders forged a rare consensus at the Summit that the bleak cyber status quo is no longer acceptable and we must take significant steps to change the tide.

The October 4th conference, organized by the Aspen Institute and CNBC, hosted current and former leaders from the White House, as well as U.S. and U.K. law enforcement and intelligence agencies, along with an extensive representation of cybersecurity companies, cybersecurity investors, and diverse private sector corporate leaders.

"We're the frog in the pot that's getting boiled," said White House cyber chief Rob Joyce. "I watch these breaches every day."

We can't continue to merely chip away at a problem that is growing exponentially. We need to act now—and collectively. Having personally wrangled cybersecurity challenges first at the Central Intelligence Agency and now across the U.S. government with our Accenture Federal Services clients, I believe the time has come for a Cyber Moonshot to secure the digital landscape in the next five years.

What we can learn from Kennedy's Moonshot is that three factors were essential to achieving success and real solutions:

1. Concerted leadership to drive unprecedented innovation
2. A specific call to action igniting unparalleled collaboration
3. Sustained investment in the technology and ingenuity needed to succeed.

[1] https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit
https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

## SO, WHAT'S NEXT?

**A real Cyber Moonshot must be an industry-led public-private partnership.** When I led a roundtable discussion on the Cyber Moonshot at the Summit, it became clear that our technology leaders, working with governments, must lead this effort.

Unlike President John F. Kennedy's Moonshot in the 1960s, when the bulk of technology expertise resided in the U.S. government, today's technical expertise lies largely in the private sector. We need to harness that energy and technology to drive this effort forward.

It's time for the leaders of global companies like Facebook, Google, Twitter, and Amazon to come together and lead the Cyber Moonshot. These organizations have begun to engage on these issues in the wake of nation states taking bolder steps to compromise the fundamentals of our democracy and public trust. Driving the Cyber Moonshot would be a powerful, and creative, next step.

**Following the hacking of emails during the 2016 U.S. presidential campaign, 40% of Americans are more cautious about what they share over email.**

This Cyber Moonshot should develop a process to ensure that organizations of all sizes implement cybersecurity basics while addressing emerging cybersecurity challenges like the Internet of Things, which will introduce more than 34 billion[2] largely insecure devices into the digital landscape by 2020. As with the Kennedy Moonshot, much of the foundational technology to deliver on a Cyber Moonshot exists, but we need to channel it toward more focused action.

Once we can assemble the right leadership across the public and private sectors, we'll need sustained investment and public awareness and support. This last element may be the most challenging to produce. We don't yet have public passion for a major cybersecurity initiative that is even close to the public excitement that fueled the Kennedy Moonshot, a key concern that was voiced at our roundtable discussion at the Summit.

But we do have growing awareness and public unease. Following the hacking of emails during the 2016 U.S. presidential campaign, Americans have made personal changes to how they interact online, with 40 percent more cautious about what they share over email, according to an Ipsos-Reuters poll earlier this year.[3]

We must, as President Kennedy did, channel that fear into a competitive edge that drives and inspires public support for a race to secure cyberspace. Our technology sector leaders are best-positioned to tap into and galvanize public support for a major cybersecurity initiative.

## WE CAN'T WAIT. THE WINDOW FOR PUBLIC SUPPORT IS CLOSING.

At the Summit, U.S. government leaders, from Sue Gordon, Principal Deputy Director of National Intelligence, to Joyce rightly warned of an emerging cyber complacency.

"We're coming to think that this is just the cost of doing business," Gordon warned, while Joyce added, "It's getting to a point where we're getting numb."

**We cannot afford to become numb as a nation because the risks are simply too great to ignore.**

## LET'S UNITE AROUND A COMMON CYBER CAUSE– THE **CYBER MOONSHOT.**

[2] http://www.gartner.com/newsroom/id/3598917
[3] http://fingfx.thomsonreuters.com/gfx/rngs/USA-CYBER-POLL/010040EN0YD/2017%20Reuters%20Tracking%20-%20Cybersecurity%20Poll%203%2031%202017.pdf