THE RED BRANCH REPORT

BECAUSE WASHINGTON IS TOO IMPORTANT TO IGNORE

July 2017

OUR VISION

We aim to bring Washington, DC to Silicon Valley.

The large Valley firms have K St. lobbyists, lawyers, and public relations professionals. The small and mid-size start-ups and entrepreneurs have nobody.

We try to fill that gap. This monthly newsletter has "news you can use" that may be important to the IT start-up sector. You may not have the resources to track it, but Washington is too important to ignore.

The US Capitol at dawn

CYBERSECURITY AND CORPORATE GOVERNANCE

Every cybersecurity consultant across America, like Red Branch, has had much the same experience. They are called in to meet with a Board of Directors who know that cybersecurity is a problem. After some investigation, they recommend changes in how the company deals with security issues – more resources; a restructuring of responsibility, perhaps; and, always, more attention from the Board.

And then ... crickets. The security posture of the enterprise may improve, or it may not. But the level of Board engagement rarely changes – or at least it rarely appears to do so.

A new bill, the "Cybersecurity Disclosure Act of 2017" (S.536), introduced by Senator Jack Reed (D-RI) aims to change that. It would apply only to publicly traded companies so it may be of little immediate relevance to Valley start-ups, but it is indicative of the direction of Congressional thinking. The bill would do two things:

> *"[G]reater transparency will cause companies to pay greater attention to their cybersecurity profile."*

First, it would require all publicly traded companies to disclose whether any member of the board of directors or general partnership, has expertise or experience in cybersecurity. Second, if no member had the requisite expertise it would require the Board to describe what steps it was taking to identify and evaluate nominees for the Board with that expertise.

Importantly, the bill would not prescribe board membership, only greater disclosure. The idea is that transparency will cause companies to pay greater attention to their cybersecurity profile and that investors will exercise discipline on publicly traded companies by avoiding investments in, or requiring a premium for purchasing the stock of, companies that have notionally inadequate Board understanding of the cybersecurity profile of their enterprise.

To be fair, that's not an unreasonable impulse. Our entire theory of securities regulation is to support transparency and let the market do the work.

But that only works when the market understands the disclosures. In the financial realm, audits that are publicly disclosed can be readily interpreted by investors. Here, that's not possible – and so the bill seeks to use a "proxy" for understanding – substituting personnel for comprehension.

Our Prediction: This bill won't become law this year. But look for it to influence a new standard of behavior. As Valley start-ups go public, they will be asked about their cybersecurity expertise at the Board level, even if this bill is never adopted. How might you respond?

IS SOURCE CODE REVIEW WORTH IT?

Nobody trusts the Russian security software maker Kaspersky Lab – at least nobody in the Federal government. Last month saw a Senate proposal that would prohibit the Department of Defense from using Kaspersky products or "interacting" with the company (whatever that may mean). Kaspersky is suspect, in American eyes, because of the CEO, Eugene Kaspersky's, former affiliation with the KGB.

Mr. Kaspersky is not taking this challenge lying down. He told the Associated Press that the company would show its source code to the US government – an effort to foster trust. "Anything I can do to prove that we don't behave maliciously I will do it," he said.

But that raises the question – is source code review worth it?

To be sure, a close review, given enough time, can likely establish that the code does what it says it does. In other words, it can establish that the code functions as an anti-virus program and it may even be able to establish that the code has no hidden offensive capabilities that can be deployed against the user.

But that's not the question here, and it is often not the question with any new code. Rather the concern is that Kaspersky's anti-virus systems are purposefully blind to certain types of intrusions – that is, Russian ones. In other words, the suspicion is that certain signatures or threat indicators were deliberately left out of the system. No amount of code review can judge that.

So ... how would you respond to similar concerns? If someone asks to review your code, how do you prove that it has everything it's supposed to have in it?

NIST CYBER AUDITS

House Republicans have introduced a proposal – to make the National Institutes for Standards and Technology (NIST) responsible for cybersecurity audits across the government. There are several serious problems with this proposal.

First and foremost, the bill asks NIST to do a job for which it is not equipped. NIST is a standard setting agency that has no operational audit experience at all.

Second, giving NIST an oversight role of any sort would erode its current standing as a neutral, technical arbiter and standard setter.

Finally, this would further diffuse and disaggregate Congressional oversight of the critical issue of cybersecurity. Congress should be moving in the opposite direction to consolidate its review as a way of asserting better direction and control of the government's response.

In late June members of NIST's Information Security and Privacy Advisory Board expressed their serious concern about changing the agency's mission. They argued that it would likely degrade NIST's ability to perform its core duties.

They're right. This is an idea whose time has not yet come.

WASHINGTON TRACKER

Our regular feature – a tracker for legislation and executive action that might be of interest to Valley entrepreneurs. With the flood of introduced bills, some new ones make the list this time around, and some older ones drop off – to return if they look to see action:

Bill # or Agency	Title	Description	Status
FCC	Repeal of Net Neutrality Regulations	The FCC has begun the process of considering how to repeal and/or replace the "net neutrality" regulations adopted by the Commission during the Obama Administraiton. The revised regulations would permit internet providers to charge variable fees to subscribers based on volume and other factors.	With the change in Administration, the revised regulations are very likely to be adopted by the Commission sometime before the end of this year. Expect the revision to be immediately challenged in Federal court, where the outcome is indefinite.
H.R. 2841 S. 1157	PATCH Act	Creates Vulnerabilities Equities Review Board to review decision on disclosure of vulnerabilities discovered by USG agencies to vendors.	Introduced May 17 in House and Senate and referred to committees; hearings may occur this year; passage unlikely.
H.R. 387	Email Privacy Act	Amends the Electronic Communications Privacy Act to require a warrant for government access to cloud-stored emails and other electronic content.	Passed Feb. 6 by voice vote in House; awaiting Senate action. Last Congress bill was killed in Senate; possible same result in 115th Congress.
S. 536	Cybersecurity Disclosure Act	Requires corporate Boards to disclose whether they have one member with cybersecurity expertise and steps they are taking to recruit expertise to the Board.	Introduced in the Senate and referred to committee. Unlikely to pass in current form.
S. 770	MAIN STREET Cybersecurity Act	Requires NIST to take into account needs of small businesses in setting NIST cybersecurity framework standards.	Introduced in Senate March 29 with bipartisan support. Unlikely to pass independently; may get added to larger bill.
H.R. 1899 S. 823	Protecting Data at the Border Act	Requires border agents to get a search warrant before searching digital devices at the border; currently no warrant is required.	Introduced in House and Senate on April 4; referred to committee; passage unlikely at this time.
S.88 H.R. 686	Developing Innovation and Growing the Internet of Things Act (DIGIT)	Requires FCC to report to Congress on IoT spectrum needs. Requires Commerce to convene working group on IoT to identify federal laws and regulations that inhibit IoT development; and examine how federal agencies can benefit from, use, prepare for, and secure the IoT. Consultation with nongovernmental stakeholders required.	Bipartisan bill introduced January 10 in the Senate; Reported to the Senate June 10 without dissent. House bill pending in committee. Good candidate for inclusion in larger bill.

Contact Us

Red Branch Consulting, PLLC
Paul Rosenzweig, Esq.
509 Ct. NE
Washington, DC 20002
O: +1 (202) 547-0660
M: +1 (202) 329-9650
VOIP: +1 (202) 738-1739
@RosenzweigP
www.lawfareblog.com
www.redbranchconsulting.com
www.paulrosenzweigesq.com

To subscribe or unsubscribe, send an email to: paul.rosenzweig@ redbranchconsulting.com

RECOMMENDED READINGS

Aaron F. Brantly, Nerea M. Cal, Devlin Winkelstein, “Don’t Ignore Ukraine, Lessons from the Borderland of the Internet,” Lawfare Blog (July 7, 2017), https://www.lawfareblog.com/dont-ignore-ukraine-lessons-borderland-internet. Hybrid war is coming – be afraid; be very afraid.

THE LAST WORD

“Station F (https://stationf.co/) is the world’s biggest startup campus. Thousands of entrepreneurs are currently moving into the new building in Paris. . . . It is a huge bet on the future of the French tech ecosystem. If things are going well for French startups, people are going to look at Station F as the physical representation of those successes " -- Romain Dillet, TechCrunch, http://tcrn.ch/2tTb9K1. And, I might add, in a post-Brexit world, a likely European destination for US companies focused on EU deployment.

PROGRAMMING NOTE

August is when Washington is asleep. Congress is away and I am too. The Red Branch Report will take a break. Our next issue will publish in September 2017.