The Demise Of HitchBOT

by Steve Brown

We read with sadness last week about the little hitchhiking robot named hitchBOT. It had successfully traveled through Germany, the Netherlands and 3,700 miles across Canada, but then met its demise in Philadelphia where someone destroyed it. The child-sized robot wearing yellow Wellington boots would sit by the side of the road with its destination clearly displayed (San Francisco or Bust!) and rely on people across the world to pick it up and carry it in their cars, on their bicycles (in Holland) or by any other means to assist it on its way. This was a social experiment by Canadian researchers and along the way, the little bot talked to the people who transported it, sent pictures home via a 3G connection and carried a GPS tracking device. HitchBOT had more than 100K followers on Facebook and won the hearts of many who took selfies with it and generally took pride in assisting it on its journey. That is, until someone felt compelled to destroy it.

Bankers may sometimes feel like their efforts at managing cyber security are as vulnerable as a little robot sitting by the side of the road. To help in this regard, FFIEC recently issued a document entitled "Cybersecurity Assessment Tool and User's Guide" to assist institutions in identifying their risks and assessing preparedness. Almost every bank has cyber security policies and procedures in place already and most have come to the conclusion that it's more a matter of when than if a data breach will occur. Therefore most are focusing on what happens once a security breach occurs. The FFIEC guide attempts to quantify and standardize this and gives banks the backup evidence that they took all the right steps, or could also show that a bank didn't take appropriate steps to mitigate risk.

So what does the guide add to the assessment process? Like BSA/AML, there are two levels of assessment - identify potential risk and then assess the specific controls and practices that are in place to mitigate that risk. The Guide calls the latter part the "Cybersecurity Maturity Level".

There are five categories that make up the identification of an institution's risk profile: (1) Technologies and Connection Types - wired vs. wireless, outsourced vs. internally hosted, cloud services etc, (2) Delivery Channels - online, mobile versus in-branch, (3) Online/Mobile Products and Technology Services - cards, P2P, fiduciary services, merchant services and global remittances, (4) Organizational Characteristics - number of employees, locations and IT considerations, and finally (5) External Threats - phishing and external attacks.

Once the risks in these areas are identified, then the institution should look at its Cybersecurity Maturity Level for 5 areas: (1) Cyber Risk Management and Oversight - the development and oversight of the enterprise-wide cybersecurity program including employee training efforts, (2) Threat Intelligence and Collaboration - identify, monitor and communicate threats to employees and vendors, (3) Cybersecurity Controls - preventative actions, (4) External Dependency Management - this is a big one for community banks in that typically there is high dependency on outside providers - oversee and manage all third parties with due diligence, ongoing monitoring and written agreements, and finally (5) Cyber Incident Management and Resilience - business continuity and disaster recovery plans - their planning, testing and implementation.

As with any risk mitigation program, the process should be ongoing and should change with the addition of new products or services, new technology and the identification of new risks. The guide can be found here.

Perhaps it was na?ve of the researchers to believe that a friendly little robot could travel unmolested everywhere. If the scientists had placed a bit more risk mitigation effort into the planning, like a stinging laser in the case of hostile attack, then perhaps hitchBOT would still be making its way around the country. For bankers at least, the regulatory community clearly feels banks must improve planning, so they have stepped up efforts to clarify expectations.

BANK NEWS

Alphabet

Google announced a major change to its operating structure, creating a holding company called Alphabet. The move will allow it to separate its web search business from other projects such as driverless cars.

Deal Done

Greece reached a final 3Y deal with its international lenders last night that will give it access to bailout money.

Devaluation

In a surprise move, China devalued its currency by the most in 20Ys; sparking fears economic growth could be slowing further in the country.

On Track

Fed Atlanta President Lockhart said he thinks the point of liftoff to raise rates is close and that conditions are no longer extraordinary.

M&A Activity

1) Bank of America will sell its appraisal management company LandSafe Appraisal to CoreLogic for an undisclosed sum.

Massive Growth

CNBC reports peer to peer online lending has grown to almost $2B in the past 5Ys, soaring 65x over that period. While it still pales in comparison to the $12T in total loans in the US, it is growing sharply nonetheless and shows some customers are interested in using such platforms to access lenders. Overall, total nonbank lending is estimated to be $15T in size.

Exam Preparatio

Bankers preparing for an upcoming regulatory exam may be interested to note a Fed report flags as high risk BSA/AML and as an elevated risk IT, cybersecurity, lengthening asset maturities (interest rate risk/liquidity) and the quality of loan growth (competitive pricing pressures).