Assessing Cybersecurity Risks

by Steve Brown

You may be surprised to find out that a new poll by Intel Security finds the average person now has 27 discrete online logins and more than 1 in 3 people forgets a password at least 1x per week. Maybe that's why studies find about 60% of people reuse passwords when going online.

Even if community banks could solve this problem in its entirety within their own organization, their own customers would still introduce significant potential cyber risk to the bank. This is one reason why regulators are highly concerned and have ramped up reviews and expectations for banks worldwide.

One suggested starting point is to incorporate the Cybersecurity Assessment Tool (CAT) from the Federal Financial Institutions Examination Council (FFIEC). The CAT is designed to help banks identify risks and determine cybersecurity preparedness. The assessment helps banks by providing a repeatable and quantifiable process, assess cybersecurity preparedness, determine risk management practices, and ensure the bank has adequate controls and strategies.

Many banks we know are working through this process or have already completed it. The tool consists of a "risk profile" part and a "cybersecurity maturity" part.

The risk profile examines the inherent risk to an institution in technology and connection, delivery channels, mobile products, and external threats. The risk level for each bank activity (from ATM services to cloud computing to wire transfers and even M&A) are detailed from least risk to most risk. A risk level is then determined for each area.

The cybersecurity maturity part includes areas of oversight, strategy and policies, IT asset management and risk management programs. Each area is then identified as baseline, evolving, intermediate, advanced or innovative. All areas of the bank are included in these tasks from the board to management to appropriate staff and committee members.

This cybersecurity assessment tool takes some time to do right and it involves all layers of the company, but we would argue it is helpful once it is completed. At a minimum, the process can help bankers think about cyber risks using a standardized format in context with the rest of the industry. This should raise internal risk awareness and improve cyber security once the process has been completed and mitigating efforts are underway.

According to the FFIEC, the assessment tool has been designed to help banks do the following: identify factors contributing to and determining the bank's overall cyber risk; assess the bank's cybersecurity preparedness; evaluate whether the bank's cybersecurity preparedness aligns with its risks; determines risk management practices and controls needed or enhancements and actions needed to achieve the desired state; and informs management and the board about risk management strategies so a plan can be created and executed upon.

No one needs extra work and the FFIEC assessment tool takes some time to complete. However, it also serves as a decent way for bankers to understand cyber risks, as you set up cybersecurity controls, monitor those controls and manage cyber-intrusion prevention programs.

No one yet has figured out an easy way to get rid of all of those 27 passwords, so holes exist all over the place. Perhaps until then, at least this cybersecurity assessment tool may keep you one step ahead of those headline-grabbing hackers as you protect your bank and your customers.

BANK NEWS

GDP Update

JPMorgan has revised its Q4 GDP forecast and increased it from 1.5% to 2.1%.

Pensions

Research finds only 13% of all private sector workers still have a traditional pension plan vs. 38% back in 1979. The pension has largely been replaced by the 401(k).

Outside Education

Research by PwC of board members from financial services companies finds 33% devote at least 16 hours per year to outside education.

Debt Ceiling

Bankers should be aware of the potential for more volatility in the coming months, as the US debt ceiling that has been suspended since late 2015 is reinstated on March 16.

Cyber Incidents

IBM cyber security research finds the most frequently occurring incident categories are: unauthorized access (45%); malicious code (29%); sustained probe, scan (16%); suspicious activity (6%); and access or credentials abuse (3%).

Board Composition

PwC research finds surveyed directors say their board has made the following changes to its composition in the past year in response to investor pressure: added a director with a specific skillset (61%); added diverse board members (46%); added younger directors (34%); removed a board member due to age (24%); and added an activist representative (17%).

College Jobs

A survey of college graduates by Gallup finds graduates who used career services at their school were 6.0x more likely to say their college prepared them for life after the university, 3.4x more likely to recommend their school to others and 2.6x more likely to donate to their alma mater vs. those who did not visit career services.

Employee Interruptions

Deloitte research finds employees now get interrupted as frequently as every 5 minutes at work, most often by work applications and collaboration tools.