FDIC CyberSecurity Assessments - What Do I need to Know?

On May 7, 2014 a webinar was presented by Federal Financial Institutions Examination Council (FFIEC) and CyberSecurity and Critical Infrastructure Working Group. The webinar included an announcement by the FFIEC that it will begin conducting vulnerability and risk-mitigation assessments, as well as regulatory self-assessment of supervisory policies and processes later in 2014.

> "These assessments will be conducted later this year and will help the FFIEC member agencies make informed decisions about the state of cybersecurity across community institutions and address gaps and prioritize necessary actions to strengthen supervisory programs," said a press release on May 7. "FFIEC members want to provide additional support to community banks, which may not have access to the resources available to larger institutions."

About now you're already thinking; here we go - another bunch of new policy, procedures and regulations we must prepare for. This article is intended to offer a perspective that hopefully dispels some of the fear and heads off rumors before they begin. Much of the fear will result from misinformation and poor definition of the key terms – Information Security and CyberSecurity.

First let's address a little history. As far back as 2011 the Department of Homeland Security (DHS) released the "Blueprint for a Secure Cyber Future", http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf. In continuing to recognize the national and economic security of the United States depends on the reliable functioning of critical infrastructure (Banking as a critical infrastructure); in February 2013, the President issued Executive Order 13636, Improving Critical Infrastructure CyberSecurity, (http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity). The executive order directed NIST to work with stakeholders to develop a voluntary framework; based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.

The Office of the Superintendent for Financial Institutions Canada released Cyber Security Self-Assessment Guidance in October 2013 for all Federally Regulated Financial Institutions. This offers an early insight into the desirable properties and characteristics of cyber security practices that could be considered by financial institutions when assessing the adequacy of their cyber security framework and when planning enhancements to same. Canadian institutions were encouraged to reflect the current state of cyber security practices in their assessments rather than their target state, and consider cyber security practices on an enterprise-wide basis.

Is cybersecurity really any different than information security?

In a recent presentation by an FDIC representative to WBA members it was noted that CyberSecurity is Information Security with a little bit of a twist. Your institution for a few years already should have had in place an Information Security Program supported by policy, procedures and technology. This program was not the final destination, it must continue to mature.

If you are a purist; you will find a way to create a difference between information security and cyber security, but if you are a practitioner they are one and the same – it is still all about protecting data/information/infrastructure - digital or not. Do we really have to care about the semantics in order to accomplish our requirements to protect our customers, our employees and our organization? Even if you argue that not all information is in computers; by today's conventions if the information isn't at the moment in a computer it probably was at one time or was more than likely generated, stored, transmitted or processed by a computer at some point in time or will be again. In the early days of our security focused past we called this discipline Data Security requiring controls to protect the

data as in Electronic Data Processing (EDP); then in the late 1970's came a broader concept of Management Information Systems (MIS); so now you needed to implement Information Security. Now the next era is upon us consisting of the wild wild west (www) made up of the Internet along with its supporting Information and Communications Technology (ICT), and the framework to protect it is being called CyberSecurity, it's really nothing new. One definition of CyberSecurity depends on the philosophy that not all information is in computers; cyber focuses on digital and as such is considered a subset of Information Security. You'll find Cyber and Information Security being used interchangeably as synonyms; *cybersecurity* seems to have become the more preferred term by the media and in many government circles. It is this author's opinion that if you build a sound Information Security Program; you will find you've also had to address most CyberSecurity concerns and as a result will pass the coming CyberSecurity Assessment requirements; albeit with a few enhancement recommendations.

But you ask; how can our institution be expected to meet CyberSecurity Assessment requirements when the FDIC has not yet released what the requirements are? If you are asking that question; it would seem you are implementing controls (Information Security Program) that was simply aimed to meet compliance, not a program based on regular assessment of risk, implementation of reasonable and commonly accepted controls in depth. Compliance to security regulations does not equal secure – we shouldn't need to be regulated to implement reasonable security requirements to protect one of our most valuable assets. We must implement improved controls because they make good business sense, are necessary and good for the communities we serve.

The terminology continues to change, but the requirements remain the same. We must protect the things of value to run our business and to that end - information is a key and the most valuable asset we have and is at the core of almost any discussion we would have surrounding servicing our customers today. The point here is – the use of "information security" and "cybersecurity" are usually interchangeable. If you use both of these terms you won't miss the point and you'll cover the entire discipline of critical asset protection.

As a critical asset, it is important to consider the value differences of information. Gartner's Doug Laney recently identified in a SearchCIO article six models that can be used to measure the value of an institution's information:

1. Intrinsic Value
   Quantify the data quality using its characteristics such as accuracy, accessibility and completeness. Data that is unique to your organization and not available to your competitors would typically have more intrinsic value to your institution.
2. Business Value
   The value is identified as a measurement of data characteristics in relation to one or more business processes in the organization.
3. Performance Value
   Consider the information based on the data's impact on one or more key performance indicators (KPIs) over time
4. Cost Value
   What was the financial cost to acquire the data or what would it cost to replace the data if destroyed in a disaster?
5. Economic Value
   How does the information asset contribute to the generating and maintaining growth of revenue in an organization?
6. Market Value
   This last model measures revenue generated by "selling, renting or bartering" corporate data, which Laney considered to be one of the best ways to value an information asset.

The organizations that achieve the best cyber defense are those that fully understand the value of information and actively manage risk from an executive level. Putting in place proactive reporting to management and the Board offer the necessary oversight to meet regulatory risk management expectations. Risk management (Figure #1) is the ongoing process of identifying, assessing, and responding to risk. Understanding the value of your institutions information assets and the systems that store, process or transmit that information is crucial to properly assessing the risks (Risk Assessment – Impact/Likelihood) that might impact it and the controls needed to prevent bad things from happening. When each banking institution prepares for the coming Federal Financial Institutions Examination Council's (FFIEC), cyber-risk assessments there are many important resources available for guidance. A key place to start refining your Information Security Program (could be known as your Cyber Security Program) would be the National Institute of Standards and Technology's Cyber Security Framework and the other free special publications created by NIST. (aka SP-800 documents) These documents can be downloaded from http://csrc.nist.gov/publications/PubsSPs.html. In order to find NIST's Cyber framework documentation visit http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. As a companion to the framework NIST released a Roadmap that discusses NIST's next steps with the Framework and identifies key areas of CyberSecurity development, alignment, and collaboration that can be found at http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

The CyberSecurity Framework is intended as a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. (Could this already be part of your institution's Information Security Program?) NIST's Framework is not a one-size-fits-all approach to managing CyberSecurity risk in your institution. A robust Information Security Program will consider elements from multiple frameworks resulting in a hybrid model, See Figure #2 for sample models. Every organization will have similar and different threats, different vulnerabilities, and different risk tolerances. How your organization implements the practices of the Framework will vary. Your Bank's individual Risk Profile will determine activities that are important to critical service delivery and as such should help make it possible to prioritize investments to maximize the impact of each dollar spent. Ultimately, the Framework is aimed at reducing and better managing CyberSecurity risks. The framework has five functions that are not intended to form a serial path, or lead to a static desired end state. Instead the functions can and should be performed concurrently and continuously to form an operational culture that addresses the dynamic CyberSecurity risk. I call this "making Information Security Part of an Institution's DNA". If it becomes part of the culture and the business, it will become natural to protect information. Ken's Golden Rue; "If every employee in an organization treats the information they work with like it is about themselves or a member of their family, they will treat it well." Additional supporting material relating to the Framework can be found on the NIST website at http://www.nist.gov/cyberframework/.

Ensure you establish an Information Security Program that is supported by one or more of the industry standard frameworks documented in Figure #2, not simply built only on meeting compliance requirements and pleasing an examiner. You can bet that the FDIC will be expecting the Information Security Programs to continue to mature, become deeper layered, integrated and illustrate a high level of resiliency that is tested regularly. The FDIC's five basic CyberSecurity Domains and key takeaways for each are listed below:

1. Cyber Risk Management and Oversight
   Governance, Resources, Training and Culture; How does the bank's staff communicate accurate and timely information about risks and the bank's ability to mitigate them, in order that management can provide the necessary oversight and prioritize resource allocations as well as inform the board of directors?

2. Threat Intelligence and Collaboration
   Intelligence gathering, Analyzing, Monitoring and Sharing; How does the bank identify and monitor cyber threats and attacks both to the individual institution and to the overall financial industry? How does the information get used to strengthen our risk assessment process – impact and likelihood?
   A few sample places include; FIPCO IT Threat Intelligence Briefings (aka IT Roundtables), WBA Technology and Security Conference, annual Verizon Data Breach Report, us-cert.gov, dhs.gov, FS-ISAC)
3. CyberSecurity Controls
   Preventative, Detective and Corrective; What technologies and proactive measures has the bank implemented to mitigate risk – firewalls/intrusion prevention, user/network monitoring, and patch/vulnerability management?
4. Eternal Dependency Management (Vendors and Third Parties)
   Connections, relationships, responsibility; How are we managing the third-party relationship risk management life cycle to ensure that our process is selecting the best third parties (not just vendors) and identifying, monitoring, and mitigating the risk that might be exposed from the type of relationship we have with third parties?
5. Cyber Incident Management and Resilience
   Detection, Mitigation, Escalation, Reporting and Resilience; How often are we testing our response plans in order to respond to a cyber-attack? Do the tests include our key internal and external stakeholders? A sampling of the ways to test incident management and resilience were recently released as "cyber vignettes". The FDIC created "Cyber Challenge: A Community Bank Cyber Exercise" (http://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html) to encourage community financial institutions to discuss operational risk issues and the potential impact of information technology disruptions on common banking functions. The Cyber Challenge provides institutions with the materials necessary to conduct short exercises or facilitated discussions around four operational risk-related scenarios. The Cyber Challenge is not a regulatory requirement; it is a technical assistance product designed to assist with the assessment of operational readiness capabilities.

"Our vision is a cyberspace that supports secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design. It is one in which we can use cyberspace with confidence to advance our economic interests and maintain national security under all conditions." — *Quadrennial Homeland Security Review Report 2010*

Doug Johnson, vice president of risk management policy for the American Bankers Association has recently noted that regulators won't be asking institutions to make changes in how they conduct their risk assessments, what they will want is to ensure that community bankers truly understand how emerging cyber-attacks could affect their business. Bottom line requirement is that we may need to go beyond just giving the pig fresh lipstick. We may be inclined to simply add some new gloss from the early days of information computing, however protecting information into the future will require that the pig gets a more robust set of wings. It means that everyone in the institution understands what might be the impact of not having a proactive information security program to implement reasonable, robust, and resilient defense-in-depth. We've been preaching the importance of oversight for several years now and a clear message from the May 7 webinar seemed to be how highly critical it is for banking leaders to increase their overall awareness of cyber-risks not just in their institution, but across the industry.

The CyberSecurity Framework is a roadmap with directions for our journey, which will continue to change as we navigate the rocky road of cyberspace, ensuring that the destination challenge for our Information Security Program may never be reached and as such will forever remain a work in progress.

Ken M. Shaurette, CISSP, CISA, CISM, CRISC, NSA IAM, FIPCO Director IT Audit and Security Services

Figure #1

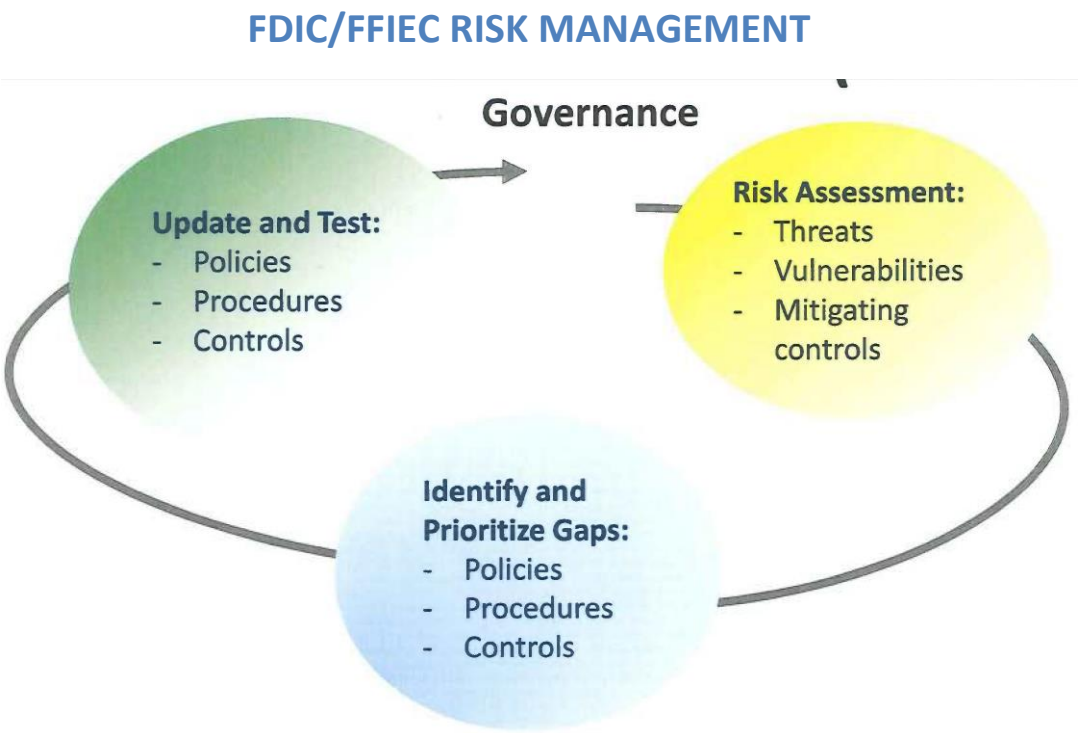

Figure #2

Information regarding Informative References described and mapped in the NIST Core Framework may be found at the following locations:

- Control Objectives for Information and Related Technology (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC): http://www.counciloncybersecurity.org
- ANSI/ISA-62443-2-1 (99.02.01)-2009, *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*: http://www.isa.org/Template.cfm?Section=Standards8&Template=/Ecommerce/ProductDisplay.cfm&ProductID=10243
- ANSI/ISA-62443-3-3 (99.03.03)-2013, *Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels*: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=13420
- ISO/IEC 27001, *Information technology -- Security techniques -- Information security management systems -- Requirements*: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534
- NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800-53r4 .

SideBAR

Cyber Crime Global Cost Is More than $400 Billion a Year

According to a report by the Center for Strategic and International Studies (CSIS), cybercrime costs businesses approximately $400 billion worldwide. The report, Net Losses – Estimating the Global Cost of Cybercrime, was sponsored by McAfee and provides the following highlights:

- In the U.S., the government notified 3,000 companies in 2013 that they had been hacked.
- The most important loss from cybercrime is in the theft of intellectual property (IP) and business confidential information, as this has the most significant economic implications. A U.S. Department of Commerce report found that IP theft (all kinds, not just cybercrime) costs U.S. companies $200 to $250 billion annually.
- Financial crime, the theft of financial assets through cyber intrusions, is the second largest source of direct loss from cybercrime. The theft of financial assets can be easiest to monetize, particularly when a cyber-criminal transfers funds from a hacked account to one they control.
- The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen. Such incidents in the last year include more than 40 million people in the U.S. This hits the areas of information value described by Laney as;
- The cost to recover from cyber-attacks, to include reputational damage, is also increasing. A 2012 survey estimated, based on the value that victims of cybercrime placed on time lost due to the incident, this amounted to an additional $274 million to the hacked company.