December 2015

Bringing Board Members Up the Cybersecurity Learning Curve

Earnings Performance Consulting

M&A Integration | Risk & Compliance

For the Intelligent Banker

2015 Intelligent Bank Management Series

The 2015 Intelligent Bank Management Series focuses on insights, strategies and development priorities for improved profitability, operating efficiency, compliance and risk management at U.S. financial institutions.

Are your Board members ready to accept newly mandated Cybersecurity accountability?

It is no surprise with the continuing revelations of compromised security credentials and identity information that Cybersecurity rises to the near top of the list of risks a financial organization must face, identify and manage.

On November 10th, the FFIEC released updated guidance with their Examination Handbook that clearly ties an expanded level of accountability in mitigating Cybersecurity threats to the institution's Executives and the Board of Directors. This is but the latest update as Regulators have delivered several pronouncements on Cybersecurity awareness in 2015, including a Cyber Assessment Tool released in the summer. The expectation by Regulators is that a Board understands and approves detailed strategies to protect data and proprietary information, accepting the fact that the US Government itself has demonstrated it cannot protect its most sensitive information. Clearly this fuels regulatory worry.

Placing accountability at the highest level is destined to change the risk narrative and presentation internally. From this expanded guidance for examiners, it is clear that IT Risk Management cannot be delegated to credentialed Information Security professionals on staff, or with your vendors, without oversight and detailed understanding and approval to the highest organizational levels. No more can an annually invited guest IT Manager parade an unopened book of project plans around the board table and receive acceptance without discussion or challenge. The key question is who is qualified on the Board to evaluate the organizational posture and

strategy with regards to Cybersecurity risk and mitigation? Who within the Board even understands the "attack surfaces"?

The Board Reality

Many recognize that Boards of Directors are typically built from community and industry pillars who have risen to a level of success and prominence that their guidance in business affairs is both welcomed and valued. While success in a field of endeavor typically involves intelligence, hard work and ethics, all valued qualities for a director, it typically does not include a detailed working knowledge or certification in Information Security.

The concepts of Information Security get very complex quickly. It would be far easier to define physical security than the more abstract concepts of logical security; everyone understands the concepts of doors and locks with card or key pad entry. A strong Information Security posture is not just good business, this is now personal to each Board Member's defined responsibility and accountability for organizational governance. While Board Members do not need to obtain a formal Information Security certification, such as a CompTIA Security+ Certificate, there is critical need for organizations to embrace the education of non-technical Executives and Board Members. We attempted to provide insight into this education process with our October paper on Cloud Computing for the Non-Technical Executive. This paper has been widely distributed. The education of Board Members must start now, and it needs to follow a formal program. We are recommending testing to validate absorption of key concepts.

Everyone benefits from the increased understanding. The expectations of risk identification by the Board will likely lead to expanded support for critical Cybersecurity mitigation efforts that may have previously been under the radar due to cost or perceived priority, in comparison to other business opportunity. In an effort to facilitate dialogue with Boards of Directors, we present:

Nine Key Concepts that Board Members Need to Understand

1. **Non-Public Private Identification Information (NPPII)** – The key requirements as established by regulation (GLBA or HIPPA) of data elements that combine to reveal information that could be used for nefarious purpose and are required to be both protected, and if breached or compromised must be revealed to impacted individuals.
2. **Data Residency** – Where does the organization's data reside, either within the control of the organization's management and organizational technology footprint, or placed outside the organization's management. Outside the organization's management would include co-location data centers, cloud computing and outsourcing.
3. **The Construct of your Network Connections** – A diagram as to how your organization is linked with the key data processing solutions that support your interactions/transactions with your customers or members.
4. **Protections Provided for Data that Resides <u>Inside</u> the Organizational Technology Footprint**
   - From outside the organization – The protection methods deployed at the perimeter where information access is enabled.
   - From inside the organizations – The internal protection methods deployed to prevent your data from being electronically compromised from within your network infrastructure.
5. **Protections Provided for Data Resident <u>Outside</u> the Organizational Technology Footprint**
   - The protection methods deployed at the perimeter to information access with vendors.
   - The protection methods employed for communication of information from your organization's technological footprint.
   - The protection methods deployed with data resident within your vendor's technological footprint.
6. **Attack Surfaces –** How nefarious individuals or organizations will attempt to exploit an opportunity, vulnerability or gullibility to gain access to restricted or confidential data. Attack surfaces are often defined as:

- Network – This includes a litany of protocol and technology acronyms (LLTD, IPv4, IPv6, TCP, SMB2 as examples) that require a Network Certification to understand.
- Encryption - The methodology utilized to change data formatting at rest or in transit to prevent data from being compromised. There are varying degrees of encryption security.
- Software - What access and harm a non-credentialed user of a software solution can obtain or perform.
- Human – How humans can be prompted, fooled or compelled to violate protocol, policy or procedure to expose confidential data and perform unauthorized transactions.

7. **Vulnerabilities** – Known opportunities for exploitation that exist with the technology components utilized within the organization's technology infrastructure.
8. **Vulnerability Tests** – The utilization of software and/or specially trained individuals employed to gain logical access to technology or data resources perceived to be secured from such unauthorized access.
9. **Security Awareness Training** – Ensuring that all staff members understand the do's and don'ts with regards to interactions in e-mails, on the Internet and with hardware and software protection mechanisms and restrictions, i.e., no thumb drives.

Clearly Cybersecurity is a moving target. Almost each week, if not daily, a new vulnerability is identified and published or a new data exposure is seemingly being revealed. Just this week, it was reported that over 1 Billion (with a "B") on-line credentials have been determined to have been compromised by just one bad actor.

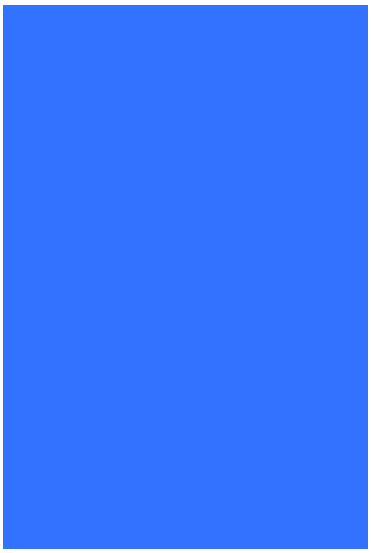
This is *the* challenge for the Chief Information Officer, the IT Manager and the Information Security Officer to keep abreast and remain vigilant to ensure vulnerabilities are identified and are remediated. We predict that as Boards understand this new level of accountability and personal risk placed upon themselves, they will require training and far more information flowing upwards from the IT organization and Vendor Management to ensure that they possess the knowledge to perform their role in the eyes (and in judgement) of Regulators.

As a leading provider of Vendor Management and Business Continuity Operational Risk solutions and consultation, CMPG is ready to lead or assist organizations detail, document, present and train Executives and Boards as to your inherent and mitigated residual operational risk, inclusive of Cybersecurity.

Give us a call to discuss how we can help you with this emerging executive educational challenge.

Jay G. Fitzhugh, Executive Consultant; jfitzhugh@cmpg.com

(443) 204-4553



To discuss the needs of your financial institution or learn more about CMPG services:

www.cmpg.com

1-800-997-2674