Risk Management for Boards
VendorInsight
White Paper

MITRATECH

BRINGING BOARD MEMBERS UP THE CYBERSECURITY LEARNING CURVE

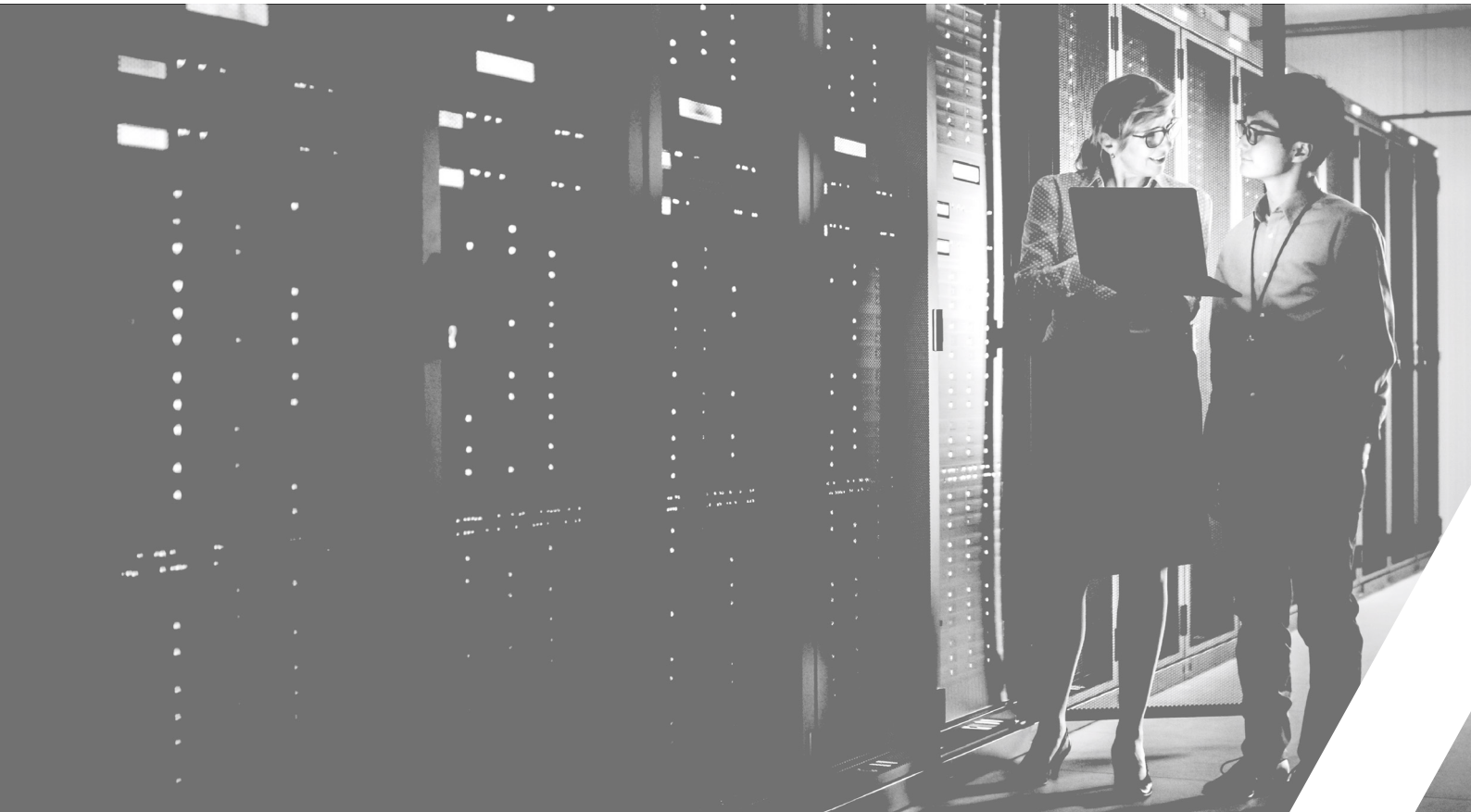
VendorInsight

INTRODUCTION

Given the continued revelations of compromised security credentials and identity information, it is no surprise that cybersecurity rises to the top of the list of risks a financial organization must face, identify, and manage.

On November 10th, the FFIEC released updated guidance in their Examination Handbook that ties an expanded level of accountability in mitigating cybersecurity threats to an institution's executives and board of directors. This is just the latest update as regulators have delivered several pronouncements on cybersecurity awareness in 2015, including a Cyber Assessment Tool released in the summer. Regulators expect 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. On account of expanded guidance for examiners, risk management work cannot be delegated to credentialed Information Security professionals on staff or with 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 on the board is qualified 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 such a level of success and prominence that their guidance in business affairs is welcomed and valued. Such successes, however do not necessarily include a detailed working knowledge or certification in Information Security.

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. The education of Board Members must start now, and it needs to follow a formal program. We recommend 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:

9 KEY CONCEPTS 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 outside the organization's management. Outside the organization's management would include co-location data centers, cloud computing and outsourcing.

9 KEY CONCEPTS TO UNDERSTAND

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 Inside 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 Outside 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.

9 KEY CONCEPTS TO UNDERSTAND

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.

CONCLUSION

Cybersecurity is a moving target. Almost each week, if not daily, a new vulnerability is identified and published or a new data exposure is revealed.

This is the challenge for the Chief Information Officer, the IT Manager and the Information Security Officer: to remain vigilant and ensure vulnerabilities are identified and are remediated. We predict that as boards understand this new level of accountability and the personal risk involved, they will require training and far more information to flow 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.

ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk & compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility and spurring collaboration across their organization.

With Mitratech's proven portfolio of end-to-end solutions, organizations worldwide are able to implement best practices and standardize processes across all lines of business to manage risk and ensure business continuity.

For more info, visit: www.mitratech.com

MITRATECH

info@mitratech.com
www.mitratech.com