333 Bush Street
San Francisco, CA 94104
(415) 263-5400
www.statefundca.com

Date: May 8, 2015

TO: MEMBERS, AUDIT COMMITTEE

I. AGENDA ITEM # AND TITLE :	Open Agenda Item 6 – Today's Technology and State Fund: Increased Risk for Boards and Leaders (Identifying IT Risks)
II. NAME AND PROGRAM:	Dante Robinson, Chief of Internal Affairs
III. ACTIVITY:	☒ Informational ☐ Request for Direction ☐ Action Proposed ☐ Exploratory
IV. JUSTIFICATION:	☐ Standard/Required Item ☒ Board Request – New Item ☐ New Topic from Staff

V. EXECUTIVE SUMMARY:

Internal Audit Management to provide IT risks training to the Audit Committee.

VI. ANALYSIS:

The presentation will cover:

- Types of Cyber Attacks.
- Recent Cyber Attacks.
- Emerging Threats.
- Counter Measures.

VII. RECOMMENDATION:

a. No action needed

VIII. PRESENTATION EXHIBITS:

a. None

IX. APPENDIX:

a. IT Risks – Cyber Attacks and Counter Measures (slides 1-11)

Today's Technology and State Fund:
Increased Risk for Boards and Leaders (Identifying IT Risks)
Audit Committee – Open Agenda Item 6
May 20, 2015

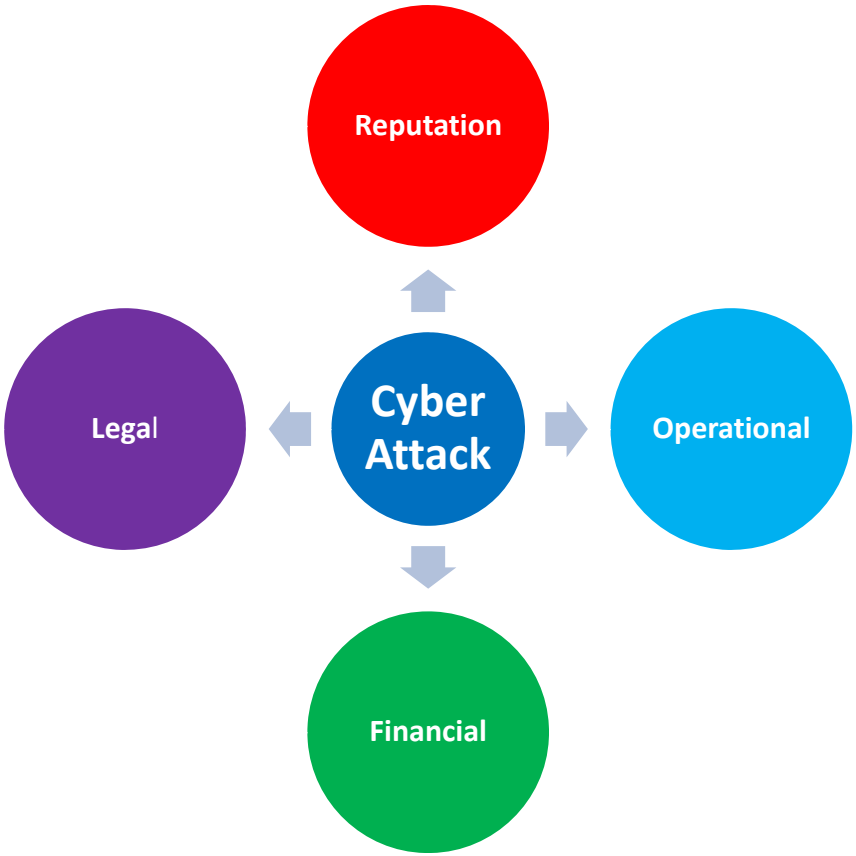
Dante Robinson, Chief of Internal Affairs

Gwillym Martin, Internal Audit Program Manager

Sanjeev Ratti, Assistant Internal Audit Manager, IT Audit Unit

Impact Matters Most

- In 60% of cyber attack cases, attackers are able to compromise an organization within minutes*.
- 15% of incidents take days to discover.*



*Verizon 2015 Data Breach Investigation Report

Top 10 WW Data Security Breaches

Records	Victim	Date	Breach / Disclosure
145 million	Ebay	May 2014	Hacking – Compromised employee log-in credentials
110 million	Target	Nov 2013	Hacking – POS Malware
100 million	Sony PlayStation	April 2011	Hacking – SQL Injection
100 million	Heartland Payment Systems	Jan 2009	Hacking – SQL Injection
100 million	TJX	Jan 2007	Hacking – Insecure Wireless
76 million	National Archives and Records Admin (NARA)	Oct 2009	Hard drive sent for repair
56 million	Home Depot	Sept 2014	Hacking – POS Malware
40 million	Cardsystems	Jun 2005	Hacking – Breached test environment containing live data
38 million	Adobe	Sept 2013	Hacking – defeated encryption on credit card data base
28.6 million	US Veterans Administration	May 2006	Stolen laptop

Source: Privacy Rights Clearinghouse - (http://www.privacyrights.org/)

Types of Cyber Attacks

Attack	Description
Compromised employee log-in credentials	This can be done through phishing, spyware that logs keystrokes, and sharing passwords. Both phishing and spear phishing are methods for hackers to obtain private information (e.g., employee credentials) by sending an imposter email that requests such information. The difference is that phishing targets a broad group of people and spear phishing targets a specific individual, often someone known to have higher level of access.
POS Malware	Point-of-sale (POS) malware is malicious software designed to steal customer payment data (e.g., credit card data). It reaches the credit card data as it is being processed, which is when the data is not encrypted.
SQL Injection	A technique whereby hackers enter structured query language (SQL) commands into log-in or other accessible fields. The intent is for the commands to allow unauthorized access to private information. If the accessible fields had strict validation criteria, it would be possible to prevent such commands from being executed.

Types of Cyber Attacks (cont'd)

Attack	Description
Insecure Wireless	A wireless network connection that does not encrypt the data sent and received through it.
Hard drive sent for repair	A hard drive contains data saved directly on a computer. The data can be accessed by individuals in possession of the computer.
Breached test environment containing live data	This is where the test environment of a software application inappropriately contained actual data taken from the production environment and was breached. The test environment is supposed to be used to verify that the code produces intended results or if the code needs to be revised. The production environment allows for actual transactions to take place and contains real data (e.g., name, social security number, etc.)
Defeated encryption	This is when encryption (masking of data so that it is protected from unauthorized access) is circumvented by computer tools.

Data Breach Commonalities

- **98%** of all data breached came from **servers**.*
  - This includes databases, web servers, and point-of-sale (POS) servers. Servers are highly susceptible because the data accessed through servers is often unencrypted, the servers may have unpatched vulnerabilities pertaining to configuration weaknesses or functionality, and server passwords may be set at defaults and easy to compromise.

- **96%** of breaches were **avoidable through key basic controls,** which can be expensive to implement.*
  - Basic control measures can be effective. This includes secure remote management tools and stronger controls when third party vendors are used for maintenance. Also important is the monitoring and restriction of access, enforcement of security policies, and monitoring data received inside and sent outside the network.

- **86%** of victims had **evidence** of the breach in their **log files**…but did not review the logs until after the breach was detected.*
  - The regular review of log files will establish an understanding of what is normal activity and identify outliers that may reflect potentially suspicious activity. Early detection of suspicious activity may prevent increased duration for breach exposure.

*2010 Data Breach Investigation Report - Verizon Business RISK Team/US Secret Service

Recent Cyber Attacks

Company	When	Breach	Causes and Counters	Source
Anthem	Dec 2014	• 78M Customers o Names o Dates of birth o Medical IDs/social security numbers o Addresses o Email addresses o employment information (including income data)	• Targeting of Network Administrators. • **Anthem declined a security audit.** • **Need for monitoring of system activity (intrusion detection system).** • **Monitor Admin Activity.** • **Encrypt data.**	http://www.securityweek.com/does-anthem-have-excuse-declining-security-audit http://www.esecurityplanet.com/network-security/5-lessons-learned-from-anthem-data-breach.html
eBay	Feb – March 2014	128M Active Users o Names o Encrypted password o Email and Physical address o Phone number o Date of birth	• Possible phishing or social engineering. • Hackers stole credentials of employees and accessed the corporate network. • **Encrypting data and increased user awareness could have helped to mitigate this.**	http://www.securityweek.com/top-data-breaches-2014 http://www.cio.com/article/2845618/data-breach/what-cios-can-learn-from-the-biggest-data-breaches.html

Recent Cyber Attacks

Company	When	Breach	Causes or Concerns	Source
JPMorgan Chase	July – Aug 2014	• 76M household customers/7M business customers o Email and mailing addresses o Home phone numbers	• A server company did not use two-factor authentication. • This enabled hackers to move around the network and access about 90 servers. • **A good intrusion detection system (IDS) could have found this sooner.**	http://www.securityweek.com/top-data-breaches-2014 http://www.cio.com/article/2845618/data-breach/what-cios-can-learn-from-the-biggest-data-breaches.html
Home Depot	Apr – Sept 2014	128M Active Users o Names o Encrypted password o Email and Physical address o Phone number o Date of birth	• Credentials of a third-party vendor obtained, likely through phishing. • Hackers gained access through an unpatched vulnerability and installed malware. • **Firewalls to block incoming and outgoing traffic could have helped.**	http://www.securityweek.com/top-data-breaches-2014 http://www.cio.com/article/2845618/data-breach/what-cios-can-learn-from-the-biggest-data-breaches.html

Emerging Threats

Threat	Description	Counter Measures	Source
Phishing and Spear Phishing	• Obtaining information by falsely identifying one's self has been around for some time. • Phishing targets a broad group of people. • Spear phishing targets an individual, often times someone with higher access privileges.	• Better email filtering before a message arrives in the Inbox. • Develop and execute a thorough security awareness program.	http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015-insider_en_xg.pdf http://www.cio.com/article/2845618/data-breach/what-cios-can-learn-from-the-biggest-data-breaches.html
Malware	• Malicious software installed on targeted systems to steal, edit, and/or sell private information. The software may also be used to impact performance (i.e., slow down or completely shut down the system). • In recent years, the attacker uses phishing to gain credentials and then installs malware to further the attack with greater consequences.	• Improve detection and response capabilities. • Firewalls can block threats.	http://www.securityweek.com/top-data-breaches-2014 http://www.cio.com/article/2845618/data-breach/what-cios-can-learn-from-the-biggest-data-breaches.html

Emerging Threats (cont'd)

Threat	Description	Counter Measures	Source
Vulnerabilities	• A flaw or weakness in a computer system or software that allows for unintended exploitation. • Examples include 2014's "Heartbleed," that allows hackers to access the memory of data servers.	• An effective patch management program will include regular updates to computer programs and systems, especially those most susceptible to threats.	http://www.securityweek.com/top-data-breaches-2014 http://www.cio.com/article/2845618/data-breach/what-cios-can-learn-from-the-biggest-data-breaches.html

References

- **Verizon 2015 Data Breach Investigations Report**
  - http://www.verizonenterprise.com/DBIR/2015/
- **Council on Cyber Security**
  - http://www.counciloncybersecurity.org/critical-controls/
- **SANS Institute**
  - http://www.sans.org/critical-security-controls/
- **Security Week**
  - http://www.securityweek.com/top-data-breaches-2014
- **CIO Magazine**
  - http://www.cio.com/article/2845618/data-breach/what-cios-can-learn-from-the-biggest-data-breaches.html