Mrs. Shereen Jones, Assistant General Manager
Group Operations and Information Technology
Jamaica National Building Society
to address
THE CYBER SECURITY AND DIGITAL FORENSICS CONFERENCE
The University of the West Indies
Thursday, November 20, 2014

PANEL DISCUSSION:
Data Protection and Cyber Security for Private and Public Sector Institutions

Salutations:

- Our Chairman, Dr William Lawrence
- Fellow presenters
- Conference Delegates
- Ladies and gentlemen…

So

INTRODUCTION

Thank you to the Mona ICT Policy Centre for presenting this second **National Cyber Security Conference** and, for inviting Jamaica National Building Society to participate in this panel discussion, ***Data Protection and Cyber Security for Private and Public Sector Institutions.***

The Art of War, an ancient Chinese military treatise, attributed to Sun Tzu, a high-ranking military general, addresses **the importance of understanding the dangers and planning to prevent attacks.** Make no mistake, ladies and gentlemen, **Cyber Crime is modern day warfare** and must be closely studied and a plan put in place to prevent attacks by cyber soldiers.

As an organization servicing 1 million customers across 30+ locations locally, with over 20 subsidiaries and affiliates spanning a wide spectrum of

financial services and other industries in Jamaica, Cayman, UK, USA and Canada JNBS places major focus on the business of cybersecurity. Safeguarding our customers' sensitive data is critical as security breaches may lead to fraud, identity theft, and loss of trust, with dire financial implications.

Cyber criminals have great interest in acquiring data of this nature.

In today's business environment – where we see mobile, cloud and social media technologies growing, coalescing and entering every phase of our lives – where we see increasing merging of the business and the personal – cybersecurity is not just a technical issue, it is a business imperative.

Today, I will share with you recent major international breaches, highlight findings from the **Cisco 2014 Annual Security Report**, consider the impact of mobile devices on corporate information security and share recommendations for IT Risk Management Resolutions. In relation to our topic, **Protection and Cyber Security for Institutions**, I will mention *three areas of focus in the JN Group*.

IMPACT OF CYBER CRIME

The global virtual environment has introduced serious threats and potential losses in the millions from aggressive cyber crime invasions and attacks. The **US State of Cybercrime Survey for 2014** reports that three in four (77%), respondents detected a security breach in the past 12 months, and more than a third (34%), said the number of security incidents detected increased over the previous year.

The survey also reported a rise in monetary losses, with an average annual loss of approximately US$415,000.

Two recent breaches demonstrate how successful cyber criminals can be:

An October 2014 **Reuters news story** reported that hackers stole contact information for **more than 80 million JP Morgan customers**. The ***New York Times*** said the breach was part of a repository of a billion stolen passwords and usernames from some 420,000 websites and was traced to a gang of Russian hackers.

Investigations revealed that the hackers obtained the website certificate for the site's vendor, allowing access to any communications between visitors and the website, including passwords and email addresses. The hackers had originally gained access to the bank's network by compromising the computer an employee with special privileges used, both at work and at home, and then moved across the bank's network to access contact data.

In May this year, the US Attorney reported that a highly organised cybercrime ring used laptops and malware to hack into financial institutions to access account information and withdraw millions of dollars from ATMs, **one of the largest bank robberies ever.**

CISCO ANNUAL SECURITY REPORT FINDINGS

The *Cisco 2014 Annual Security Report* presents **three key findings**:

1. Attacks against infrastructure are **targeting significant resources across the Internet**. Malicious exploits are gaining access to web hosting servers, name servers, and data centers.
2. Malicious actors are using trusted applications **to exploit gaps in perimeter security**. Spam continues its downward trend, although the proportion of maliciously intended spam remains constant.
3. Investigations of multinational companies show **evidence of internal compromise**. Suspicious traffic is emanating from their networks and attempting to connect to questionable sites.

Another area which is becoming more and more critical is **the impact of mobile devices on corporate information security**. In 2013, software

technology firm, **Checkpoint,** conducted a global survey of **790 IT professionals in the United States, Canada, United Kingdom, Germany, and Japan.**

Key findings of the survey include:

- Increasing numbers of **mobile devices connect to corporate networks**, with more than 93% of the survey respondents connecting and 675 allowing personal devices to connect…
- 45% have more than **five times as many personal mobile devices** as they had two years ago, an increase from 36% last year

The effect of cybercrime on mobile devices can be as devastating as an attack on a computer mainframe. It is essential, therefore, that businesses consider and include mobile devices in an effective Cyber Security Plan.

Gartner speaks to the nexus of forces – referring to the coalescence of mobile, cloud, social media and big data. While this nexus creates some amazing opportunities for new products and services – even new industries, it also creates significant challenge for those involved in security. And it places significant responsibility on all users of this technology.

IT RISK MANAGEMENT RESOLUTIONS

Dark Reading, one of the most widely read and trusted cyber security news sites on the Web, recently published a list of the **top five IT Risk Management Resolutions for 2014**. Of which I will briefly mention 3:

Resolution #1: **Risk Management Analysis** should be a vital area of focus for IT security professionals. The potential risks and threats faced by organisations should be keenly considered, analysed and managed on a daily basis, with policy and guideline requirements and system changes put

in place to minimize attacks. The risk management function needs to be tuned for greater flexibility and response and evolve from focusing on static border protection and access control. That may require increasing the resources whose primary daily responsibility is focused on risk management analysis and who monitor, conduct training, testing and updates, as required.

Resolution #2: Use of Data to Assess Risks
Data mined from security technologies and IT infrastructures are equally important to validate that the assumptions made when answering questions are truly valid.

Resolution #3: Collaborate With Business Users
Increased collaboration between businesses IT professionals and business users, to ensure closer alignment between IT's management of risk and business objectives.

Jamaica National Building Society

Information Technology Security Plan

At the end of the day, an effective **Information Technology Security Plan** must be underpinned by **a solid risk management-based multi-layered security framework**, the use of data to support analysis and, increased collaboration between IT professionals and business users, all areas of focus at Jamaica National, which helps to ensure that doing business with us is safe and secure. Other safeguards employed by the Society include **education and training** and **securing computers, equipment and digital assets**.

Education and Training:

JNBS staff members are trained to help to protect against cyber criminals. These range from **User ID and password requirements, PC, laptop and mobile user security, incident reporting, internet access guidelines and increasing awareness regarding phishing techniques, social engineering, hoaxes and spam.**

At JNBS our members' safety is very important to us, and, we regularly inform and update our employees and customers regarding security awareness and steps to prevent ATM and debit card fraud.

Securing Computers and Equipment

All software is continuously updated and security checks conducted on all corporate websites and applications on a regular basis to further strengthen and enhance our IT security.

Critical data is reliably backed up and there is an effective process in place to recover data. A computer security incident response team is in place to quickly investigate, identify, address and document any security issues that may arise.

CONCLUSION

Ladies and gentlemen, in this increasingly technological world, we must wage war and become even more vigilant about the necessity for data protection and cyber security for private and public sector institutions.

The challenges of cybercrime can be overwhelming for any single entity. We must ensure that the public and private sector – Government officials, business leaders, security professionals and utilities, work together to share intelligence and best practices and to address the many issues to provide an effective response.

The **Global State of Information Security Survey 2014** reports that a high percentage of companies with high-performing security practices collaborate with others to share information and respond more effectively to threats and attacks. The report also encourages participating in Information Sharing and Analysis Centers (ISAC) forums, particularly for the financial services and technology industries.

Data Protection and **Cyber Security for Institutions** must be **informed by international standards and best practices in information technology security**. Risk management analysis, the use of data and increased collaboration, through conferences and workshops such as this, will encourage greater regional collaboration and sharing of facts and statistics about cybercrime.

As we seek to take advantage of some of the economic benefits to be derived from the explosion in and coalescence of various technologies (mobile, cloud, social media, big data, etc.) our organizations must balance the economic imperative with the social and moral obligation to safeguard our assets and those entrusted to our care. Cybersecurity is about risk management. It needs to be a part of corporate strategy and culture as we seek to deliver to customers, clients and constituents results that are effective, efficient and secure.

Ladies and gentlemen, I leave you with a quote from the Art of War, "**If *you know your enemies and know yourself, you can win a hundred battles without a single loss***."

Mrs. Shereen Jones
Assistant General Manager
Group Operations and Information Technology
Jamaica National Building Society
November 20, 2014