Why CEOs must take cyber security seriously

Presentation to the Jamaica Institute of Financial Services/Jamaica Bankers Association

Anti Fraud Committee

“Fraud: Strengthening our Defense”

July 13, 2017

julianjayrobinson

julianjrobinson.com

julianjayrobinson

julianjay

Julian J. Robinson MP

Opposition Spokesman on Information & the Knowledge Economy

Why is cyber security a big issue for financial services companies

- Cyber attacks against financial services cost consumers £8bn in 2016 in the UK – ThreatMetrix 2017
- Researchers found that 38% of all financial threat detections were against corporations rather than consumers. Even though such attacks are harder to carry out and take longer to prepare, they yield a much higher profit. The financial threat space is still 2.5 times bigger than that of ransomware – Symantec 2017
- Average cost of a data breach to a company has risen from $5.85M in 2014 to $7.35M in 2017 – IBM/Ponemon Institute 2017

Jamaica lost US$100M to cyber crimes in 2016

Jamaica lost US$100m to cyber crimes during 2016

Friday, May 26, 2017

Tweet

KINGSTON, Jamaica – The National Security Council (NSC), in a meeting yesterday, learnt that Jamaica, in 2016, lost approximately US$100 million to cyber-criminal activity.Head of the Computer Incident Response Team (CIRT), Dr Moniphia Hewling revealed the data during her presentation to the NSC while

The 5 highest impact categories of cyber crime

- Impairment of asset value: cyber criminals steal intellectual property or sensitive information.
- Impairment of the back system: cyber criminals steal money / commit cyber fraud.
- Impairment of automated controls: cyber criminals render seemingly effective IT controls ineffective by simply bypassing them.
- Risk of contractual obligations: fines due to data privacy, breach notification act or regulators.
- Continuity risk: cyber criminals sabotage (on purpose or by accident) the IT-environment and shutdown primary business process. Depending on the nature of the business and size of the disruption, your organization may not be able to recover.

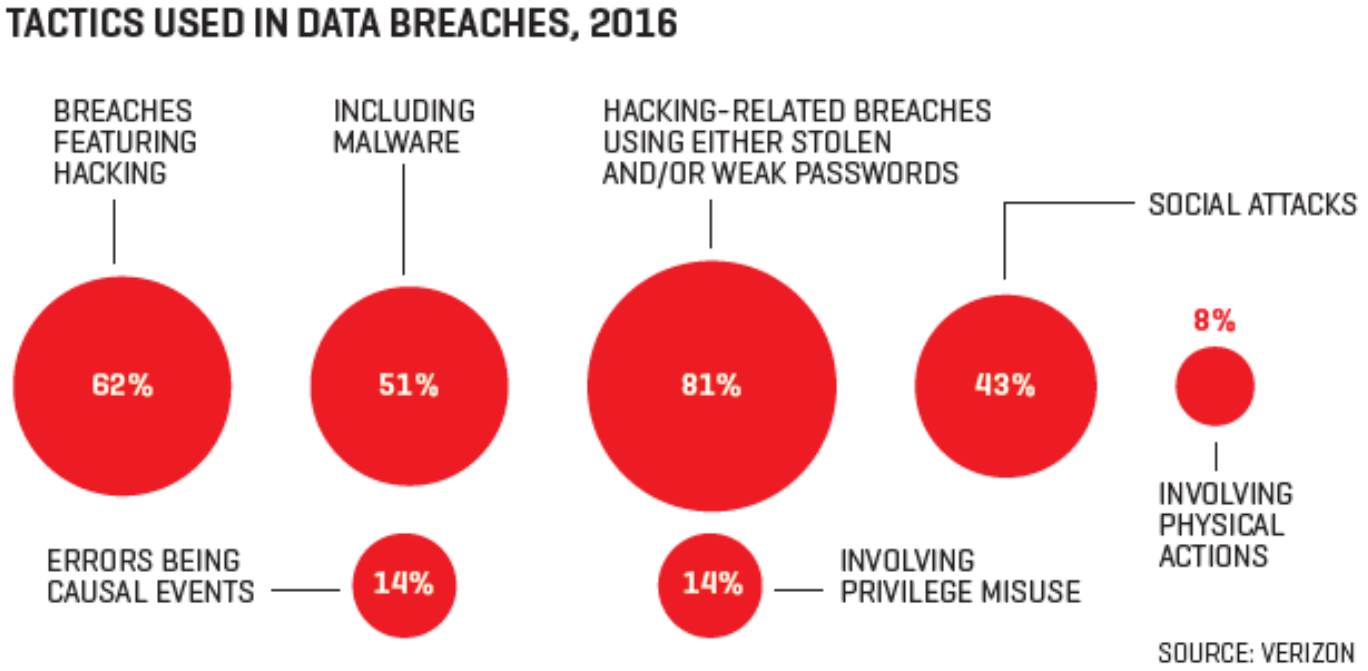
Source: KMPG

Globally, most companies pay insufficient attention to cyber security

- 56% of the companies surveyed pay insufficient attention to cyber security
- Only a quarter of the companies dedicate at least a paragraph to cyber security in their annual reports
- Less than 20% of companies consider cyber risks a boardroom responsibility

Source: KMPG 2017 – research into cyber security reporting in 800 companies across 28 countries

Combatting cyber crime is as much technical as it is human relational



<u>Two of the most frequent causes of hacking</u>

- Employee clicks on booby trapped link or attachment that seemingly comes from a legitimate source
- Someone steals an employee's login credentials

Critical management considerations in handling cyber attacks

- Establish an Incident commander
  - Responsible for managing during an attack
- Should be the CIO (Chief Information Officer) and CISO (Chief Information Security Officer)be the same person?
- Who should the CISO report to? CIO or CEO
- Is your business insured against cyber attacks?

What should you do to ensure that you are protected

- Play an active role in the legislative process – form a working group to review legislation
  - Cybercrime Act of 2015
  - Data Protection legislation coming
- Support the implementation of the National Cyber Security Strategy

NATIONAL CYBER SECURITY STRATEGY

GOVERNMENT OF JAMAICA

Components of the National Cyber Security Strategy

Technical measures

Human resource and capacity building

Legal and regulatory

Public education and awareness