Do the Neutron Dance with Cybersecurity

Lucas Anderson
TASB Risk Fund
May 1, 2020

TASB™ RISK FUND

Agenda

- Cybersecurity overview
  - Cybersecurity statistics
  - Attack Trends
  - Coronavirus related attacks
  - Remote working challenges
- Handling Sensitive Data
- Cybersecurity Coverage
  - Types of coverage and incidents
  - Cybersecurity insurance trends
- Other TASB cyber offerings

TASB™ RISK FUND

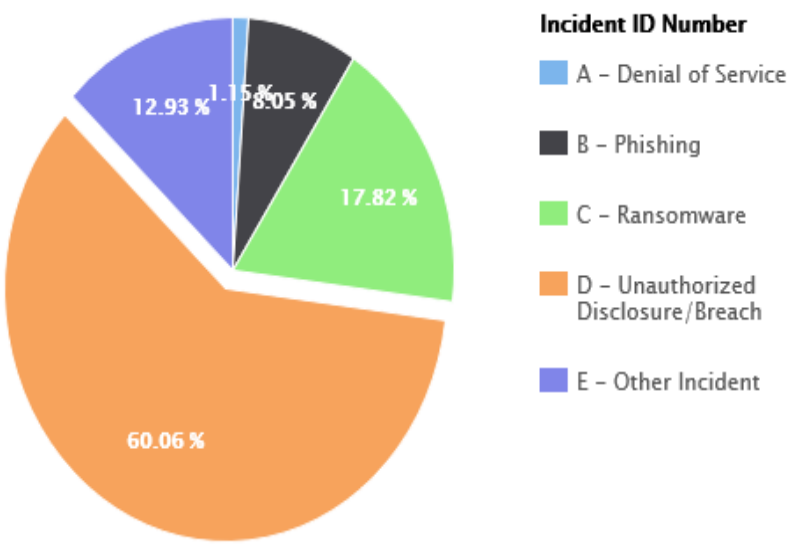
Cybersecurity Statistics

- Annual Losses in 2015 - $3 trillion Dollars
- Annual losses by 2021 - $6 trillion Dollars
  - More profitable than the global trade of all major illegal drugs
- Greatest transfer of economic wealth in history
- Fastest growing crime in the US
  - Government declared cyberthreat a national emergency
- Spending on cybersecurity $1 trillion from 2017-2021
- 1.5 Million vacant cybersecurity positions worldwide
- Half of all cyberattacks target small business and governments

TASB™ RISK FUND

Statistics from Cybersecurity Venture – Cybercrime Magazine 2019 Annual Report

Cybersecurity Statistics (cont.)



- 348 publicly disclosed incidents against schools in 2019
  - 3x the amount from 2018
  - 1/day in 2019
- As of 2016 education is the most targeted sector for ransomware
  - Incidents doubled from 2018-2019
- Millions of taxpayer dollars lost in business email compromise (BEC)
  - Highest loss - $3.7 million dollars – Scott County Schools, Kentucky

TASB™ RISK FUND

Cybersecurity Attack Trends

- Fraudulent Instruction
  - a party impersonating an individual or company through **fraudulent** emails or phone calls to deceive you into giving away private information or funds via wire transfer.
- Business Email Compromise (BEC)
  - a form of cyber crime which use email fraud to attack commercial, Government and non-profit organizations to achieve a specific outcome which negatively impacts the target organization.

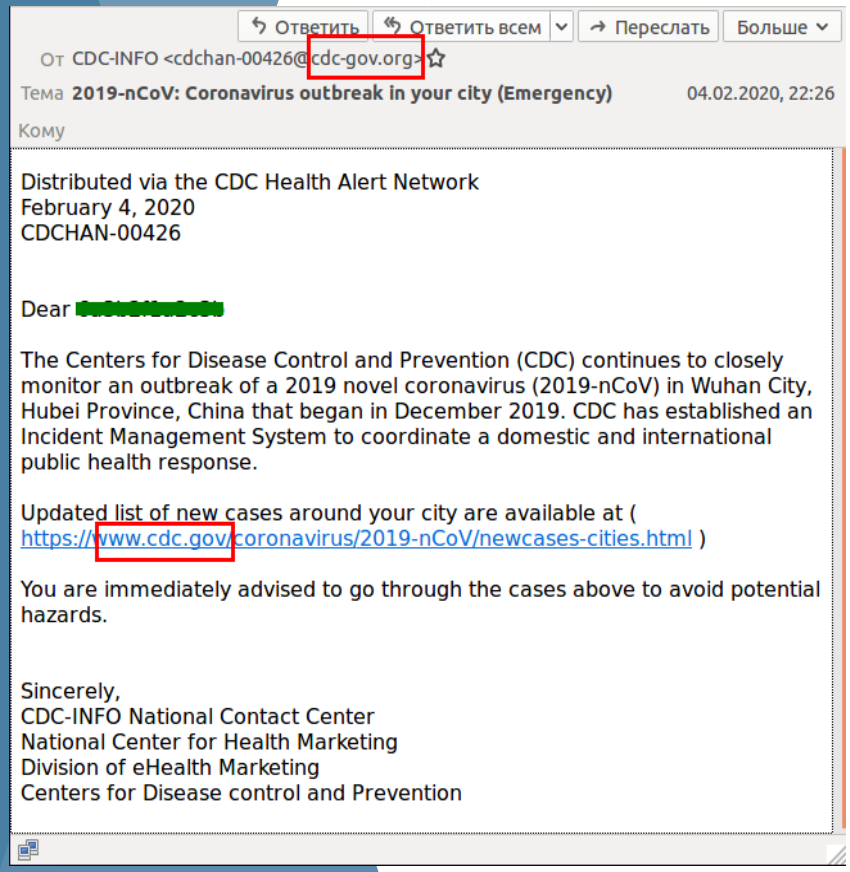
TASB™ RISK FUND

Coronavirus Scams

- WHO Scam
  - Contains malicious attachment
  - Includes a keystroke logger
  - Steals passwords and financial information

TASB™ RISK FUND

Coronavirus Scams (cont.)



Ответить | Ответить всем | Переслать | Больше

От CDC-INFO <cdchan-00426@cdc-gov.org>

Тема **2019-nCoV: Coronavirus outbreak in your city (Emergency)** 04.02.2020, 22:26

Кому

Distributed via the CDC Health Alert Network
February 4, 2020
CDCHAN-00426

Dear [redacted]

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at (https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above to avoid potential hazards.

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

- CDC Scam
  - Email from a fraudulent representative
  - Purported safety measures
  - Directs you to create account
  - Requests personal information

TASB™ RISK FUND

Remote Work Challenges

- Unsecured WiFi
  - Can allow malicious actors access to your network
  - Home and public wi-fi
- Access to equipment
  - Children and other family members
    - Digital natives
- Remote Software Platforms
  - Zoom Bombing
  - Unsecure Meetings

TASB™ RISK FUND

Remote Work Challenges

- VPN
  - IT teams need to ramp up capacity
  - Multi-Factor authentication
- Fraudulent IT Scams
  - Malicious actors know staff work remotely
  - Impersonation of IT teams
  - IT does not call unsolicited

TASB™ RISK FUND

Handling Sensitive Data

- Sensitive Data
  - PHI
  - PII
  - Tax information
- Other personal/financial data
  - Passwords
  - Routing numbers/Bank Accounts
- Prime targets for hackers!
  - Lowest hanging fruit

TASB™ RISK FUND

Handling Sensitive Data (cont.)

- Data Classification
  - Public/Proprietary/Sensitive
  - Network segmentation/segregation
- Access Policies
  - Network access
  - Acceptable use policies (AUPs)
  - Physical security policies
- Data Loss Prevention
  - Configure Email Security Appliances (ESAs)

TASB™ RISK FUND

Types of incidents covered

- Ransomware
- Fraudulent Instruction
- Regulatory Proceeding
- Unauthorized Access or Use of Computer Systems
- Unauthorized Disclosure of Data (phishing, spoofed emails)
- External Hack (virus)
- Stolen or Lost Technology Device
- Access to Unsecured Electronic or Physical Records

TASB™ RISK FUND

TASB Fund Claims

- 2014-2020
- 6 External Hacks
- 7 Fraudulent Instruction
- 20 Phishing Email Attacks
- 15 Ransomware Attacks
- 4 Stolen Technology/Device
- 9 Unsecured Electronic Records
- 3 Unsecured Physical Records

TASB™ RISK FUND

Other TASB cyber offerings

- Legislative Updates:
  - SB820 – Cybersecurity Plan
  - HB3834 – Annual Cybersecurity Training
- Custom, district specific, training
  - Based on staff needs
  - Ongoing claim patterns
- Additional Information:
  - https://www.tasbrmf.org/member-service-center/risk-solutions/special-risk-services/data-privacy-and-cybersecurity.aspx

TASB™ RISK FUND

Questions?

Lucas Anderson, Privacy and Cyber Risk Consultant

- 512.505.2893
- Lucas.Anderson@tasb.org

TASB™ RISK FUND