The CPAs role in maintaining security and promoting data privacy

CPAs 2.0: Keeping Pace with the Business Transformation
14 June 2019

Cybersecurity Incidents

Impact of Cybersecurity Breaches

Role of CPAs in Mitigating Cyber Attacks

Tips to Protect Oneself from Cyber Threats

Q&A

Contents

1

Cybersecurity Incidents

Cyber attacks are headline news everywhere…

LinkedIn Lost 167 Million Account Credentials in Data Breach (2016)

A hacker, who goes by "Peace," claims to have acquired a total of 167 million of the leaked login credentials and is selling 117 million email and password combinations on a dark web marketplace, Vice Motherboard reports. The going rate for the loot is five Bitcoins, or about $2,300.

fortune.com/2016/05/18/

UBER CONCEALED CYBERATTACK THAT EXPOSED 57 MILLION PEOPLE'S DATA

Published on November 21, 2017.

3

FORTUNE

Yahoo Agrees to $50 Million Settlement for Those Affected by...

Yahoo Agrees to $50 Million Settlement for Those Affected by the 2013 Data Breach

LinkedIn

Cyberattack hits 10,000 patients' health data

Ransom demanded from CUHK medical faculty as other victims come forward

Danny Mok
danny.mok@scmp.com

PUBLISHED : Wednesday, 06 August, 2014, 4:50a
UPDATED : Wednesday, 06 August, 2014, 4:50am

The cyberattack targeted the faculty's Centre for Liver Health and Institute of Digest Disease at the Prince of Wales Hospital in Sha Tin. Photo: Sam Tsang

Chinese University's Faculty of Medicine has fallen victim to a new wave cyberattack, with data on more than 10,000 patients hidden from view ar ransom demanded to decrypt it.

The attack targeted the faculty's Centre for Liver Health and Institute of Digestive Disease at the Prince of Wales Hospital in Sha Tin. A faculty spokeswoman said last night that it was operating as normal and patient

British Gas leak exposes customer data: Change your password now

…tomers should change their passwords now as the energy giant has …red a "data leak" last night affecting just over 2,000 customers.

…er says the email addresses and passwords of 2,200 of its customers were …st night, but it adds that payment details, such as bank account or credit …ere not at risk.

An email to the 2,200 affected customers reads: "I can assure you there has been no breach of our secure data storage systems, so none of your payment data, such as bank account or credit card details, have been at risk. As you'd expect, we encrypt and store this information securely."

The email addresses and passwords, which British Gas says were removed on Wednesday evening, were displayed on Pastebin, a temporary text uploading website, and were discovered during routine online checks. British Gas won't however confirm exactly which customers are affected or if the leak extends to its 'white label' brand, Sainsbury's Energy.

Related MSE Guides

Cheap Energy Club Homepage Redirect

Cheap Gas & Electricity
Compare now to save £100s

30 Ways to Stop Scams
As scams get clever, we need to too!

Forbes Billionaires Innovation Leadership Money Consumer Industry

Marriott Breach Exposes Far More Than Just Data

David Volodzko Contributor
Manufacturing
I am an editor at the technology and information company Brightwire.

Cyber attacks are headline news everywhere…

ABS-CBN shuts down 2 online stores amid data breach

213 customers likely affected

By: Miguel R. Camus - @inquirerdotnet Inquirer Business / 02:25 PM September 19, 2018

ABS-CBN Broadcasting Center in Quezon City (Photo by GRIG C. MONTEGRANDE/Philippine Daily Inquirer)

Media giant ABS-CBN Corp. said Wednesday it temporarily shut down two online stores that were targets of a data breach that may have exposed the personal and financial information of over 200 customers.

ABS-CBN however said in a statement that the incidents involving ABS-CBN Store (**store.abs-cbn.com**) and the UAAP Store (**uaapstore.com**) were isolated and did not affect its other digital properties. The websites were shut down at 9:30 a.m. on Wednesday.

LATEST STORIES | MOST READ

BUSINESS
Philweb decries Pagcor's 'bias' for competitor
JANUARY 13, 2019 08:46 PM

SPORTS
'Family-oriented' June Mar Fajardo taught by mom to always stay awa from trouble
JANUARY 13, 2019 08:44 PM

SPORTS
Chooks-to-Go gives financial aid to Sisters of

Wendy's PH website hack exposes thousands of personal data

By CNN Philippines Staff
Updated 07:44 AM PHT Wed, May 9, 2018

Like Share Christine Joy and 2.6M others like this.

Jollibee ordered to suspend online delivery system over privacy concern

By: Roy Stephen C. Canivel - @inquirerdotnet 08:27 PM May 08, 2018

people in the online delivery database of popular fast ods Corp. (JFC) are in "high risk" of being exposed to ilities in the system although its database has not ational Privacy Commission (NPC) said.

LATEST STORIES | MOST READ

SPORTS
Former NBA star pleads guilty in college basketball bribery sche

NEWSINFO
MWSS administrator: N need to resign for now

NEWSINFO
3 private armed group members yield in Masbate

NEWSINFO
12-year-old girl 'raped and killed' by brothers, uncle in India

NEWSINFO
New Zealand gunman 'faces isolation' due to prison dangers

Over 900,000 affected by Cebuana Lhuillier data breach

Arianne Merez, ABS-CBN News

MANILA (2nd UPDATE)—More than 900,000 clients of Cebuana Lhuillier were affected by a breach that may have compromised their personal data, the local pawnshop said Saturday.

The figure represents about 3 percent of its total clientele, Cebuana Lhuillier said.

Information that could have been compromised includes birth dates, addresses, and sources of income, the company said in a statement.

Cebuana Lhuillier bares data breach, tells clients to secure accounts

Facebook data breach affected 755,973 users in the Philippines

by Louie Diangson - October 18, 2018

Like 562 Share 1046 Tweet 27

On October 17, 2018, the National Privacy Commission Facebook to action regarding recent data breach that around the globe, including 755,973 users in the Phil

NEWSBYTES PHILIPPINES

HOME | I.T. NEWS | BUSINESS I.T. | RESEARCH REPORTS | E-SECURITY | E-LEARNING | GADGETS | MORE POSTS | Search

Cathay asked to explain data breach that affected 102,209 PH users

Cyber attacks are headline news everywhere…

INQUIRER.NET

Cyberattacks in PH surged in Q2

By: Miguel R. Camus - @inquirerdotnet

Philippine Daily Inquirer / 05:05 AM August 14, 2018

Cyberattacks in the Philippines increased over the last three months, landing the country among the top 10 most attacked for the second quarter of 2018.

According to cybersecurity company Kaspersky Lab, there were some 10.6 million web infections detected in the country during the period, causing the Philippines to climb to ninth most-attacked during the period, or up eight notches in just three months. In the first quarter, the company recorded 5.67 million infections.

BusinessWorld

ECONOMY

Philippines no. 9 on most-attacked list online — Kaspersky Lab

August 13, 2018 | 9:39 pm

Ten biggest breach incidents reported, August 2018

Company/Organization	Number of Records Stolen	Date of Breach
Yahoo	3 billion	August 2013
Equifax	145.5 million	July 2017
eBay	145 million	May 2014
Heartland Payment Systems	134 million	March 2008
Target	110 million	December 2013
TJX Companies	94 million	December 2006
JP Morgan & Chase	83 million (76 million households and 7 million small businesses)	July 2014
Uber	57 million	November 2017
U.S. Office of Personnel Management (OPM)	22 million	Between 2012 and 2014
Timehop	21 million	July 2018

What types of data are usually stolen?

Business

Reddit (June 2018)
Content Aggregator

- ❑ Hackers gained access to an old database of users

Equifax (July 2017)
Information Solutions Provider

- ❑ Affected 143 million consumers in the U.S.
- ❑ Data exposed: Names, Social Security numbers, birth dates, and addresses

Medical/Healthcare

SingHealth (July 2018)
Medical/Healthcare Service Provider

- ❑ Nonmedical personal data of 1.5 million patients reportedly accessed and copied.
- ❑ Includes national ID, address, and birth date and the outpatient medical data of 160,000 patients.

Hong Kong Department of Health (July 2018)
Federal Agency

- ❑ Ransomware attack that rendered its systems inaccessible for two weeks starting 15 July.

Banking/Credit/Financial

JP Morgan Chase & Co. (October 2014)
Credit Service Provider

- ❑ Estimated 76 million households and 7 million small businesses was compromised
- ❑ Included names, addresses, phone numbers, email addresses, and others.

Source: https://www.trendmicro.com/vinfo/be/security/news/cyber-attacks/data-breach-101

Data Privacy Law in the Philippines

NATIONAL PRIVACY COMMISSION

An act protecting individual personal information in information and communications systems in the government and private sector

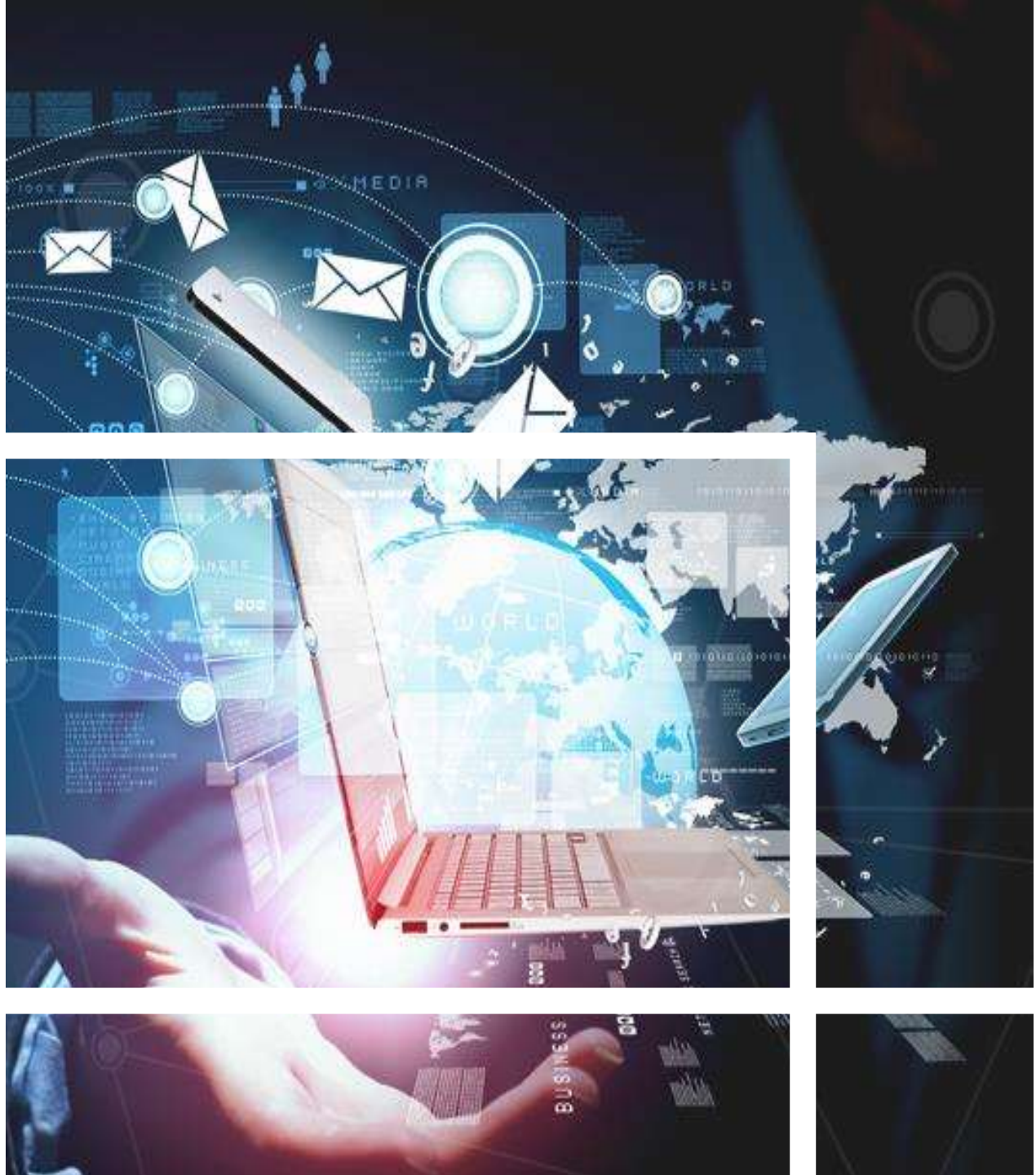
Raymund Enriquez Liboro
Privacy Commissioner and Chairman

Republic Act 10173 – Data Privacy Act of 2012

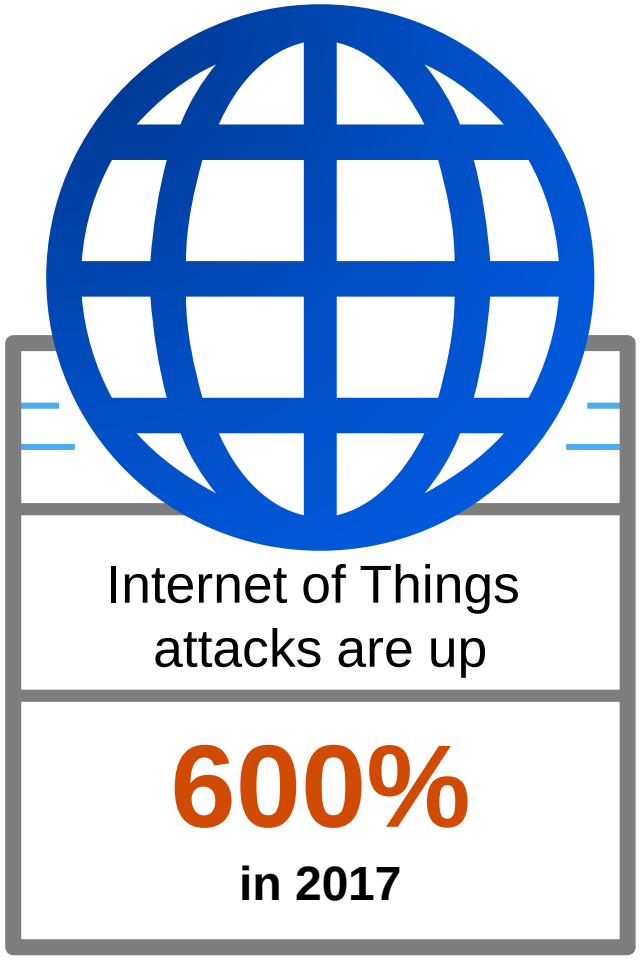
https://www.privacy.gov.ph

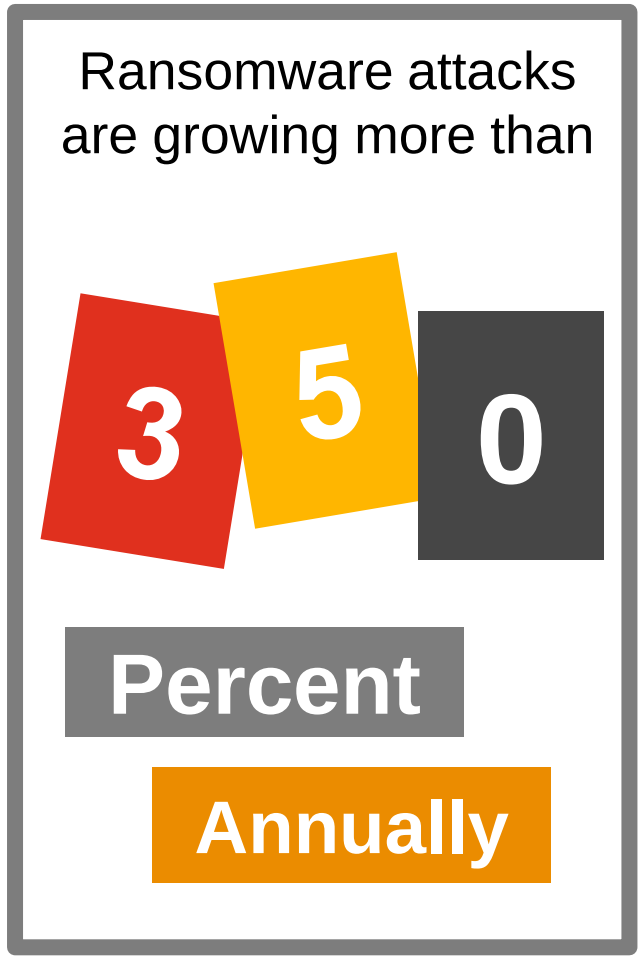
2

Impact of Cybersecurity Breaches



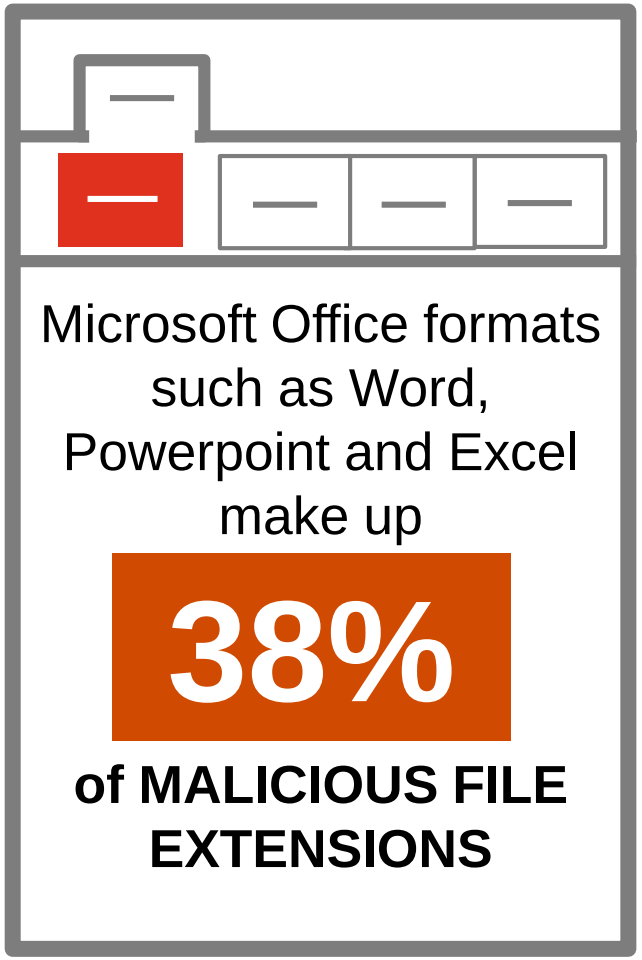
Data breaches by the numbers





Source: *Facts and figures obtained from varonis.com/blog/cybersecurity-statistics

Where do Cyber Attacks Come From?

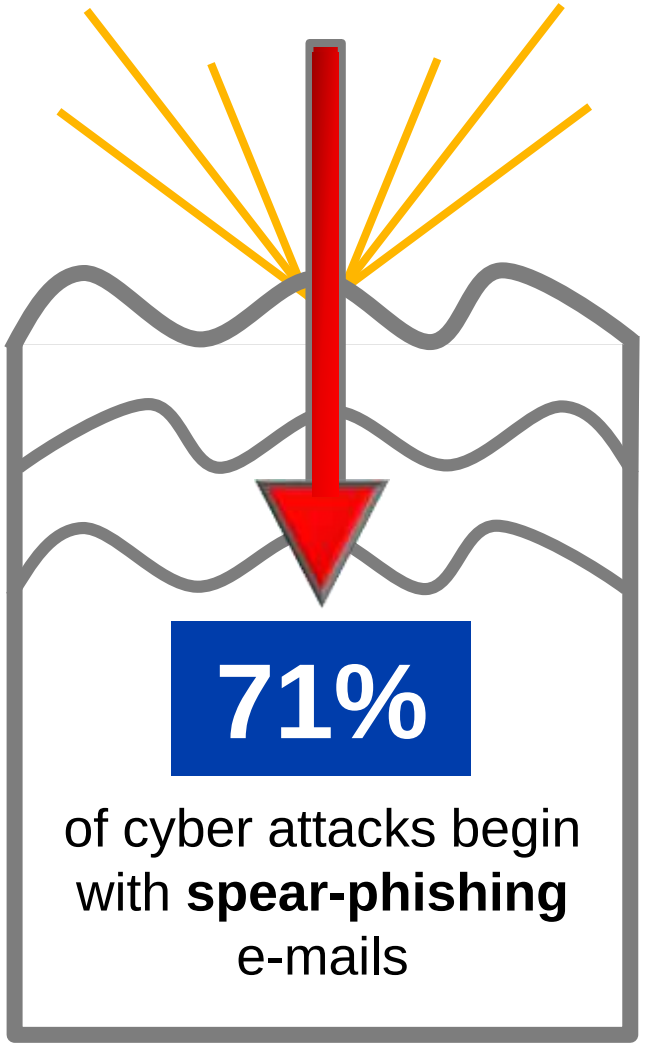


Microsoft Office formats such as Word, Powerpoint and Excel make up

38%

of MALICIOUS FILE EXTENSIONS

Sources of cyber attacks in 2017

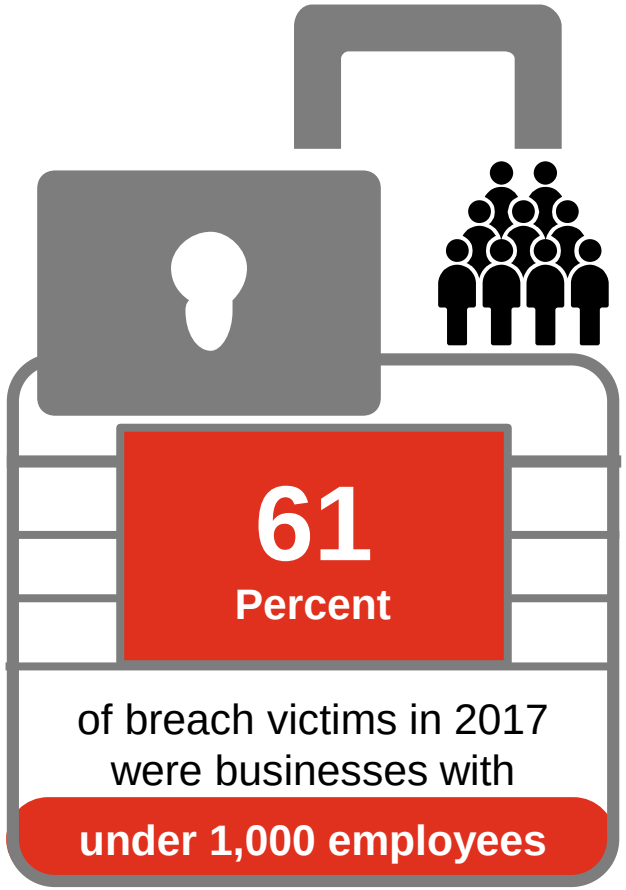


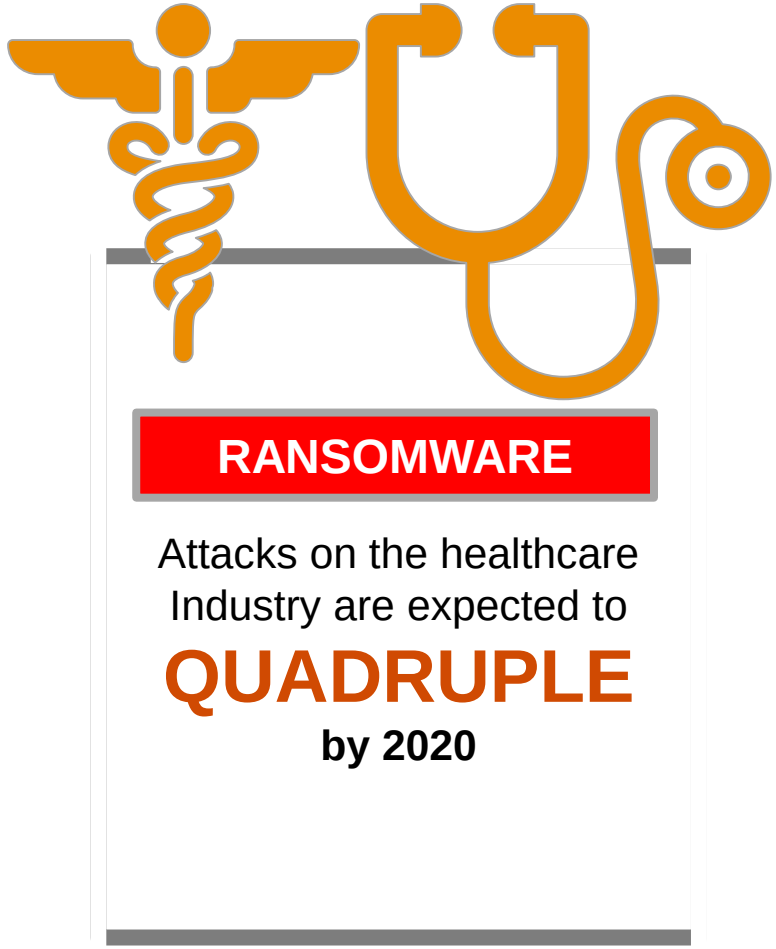
71%

of cyber attacks begin with **spear-phishing** e-mails

Source: *Facts and figures obtained from varonis.com/blog/cybersecurity-statistics

Who are affected by these data breaches?





Source: *Facts and figures obtained from varonis.com/blog/cybersecurity-statistics

Who are affected by these data breaches?

The **FINANCIAL SERVICES INDUSTRY** sees the highest cost of cyber crime.

It costs the average business

$18.3 MILLION

Source: *Facts and figures obtained from varonis.com/blog/cybersecurity-statistics

Who are affected by these data breaches?

How often are Phishing e-mails clicked?

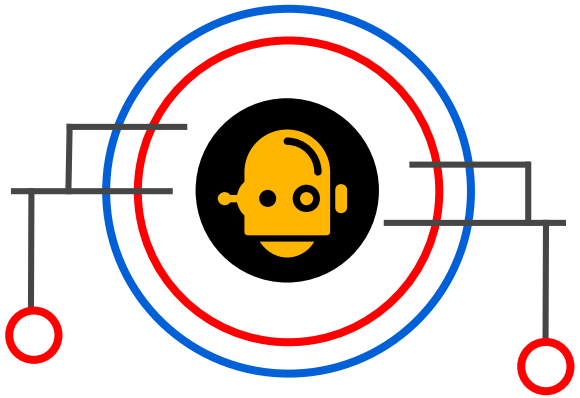
52% All successful phishing emails are clicked on within **one hour** of being sent

25% Clicks occurred within **five minutes**

11% Clicks occurred within **one minute**

Source: *Facts and figures obtained from varonis.com/blog/cybersecurity-statistics

What is the cost of data breach?



The average cost of a malware attack on a company is

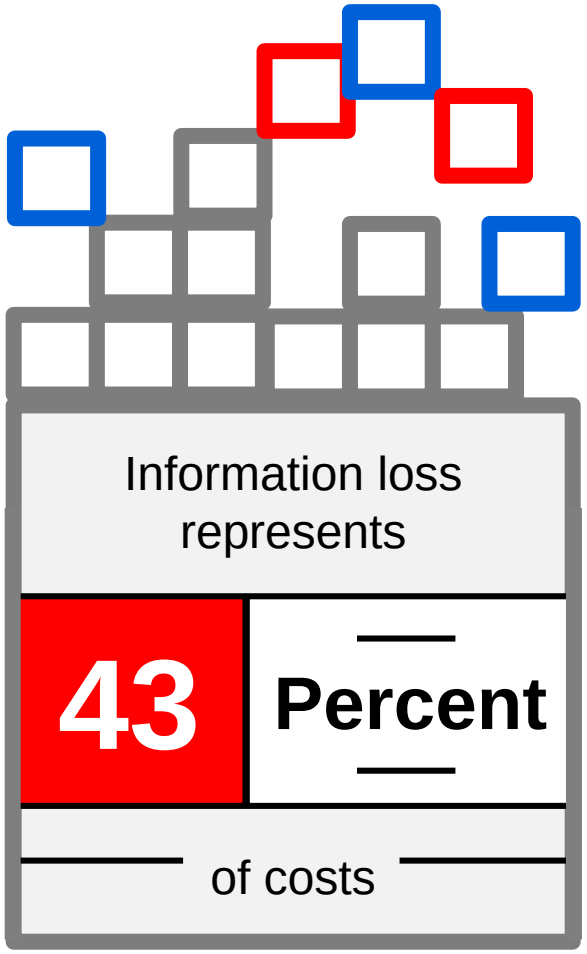
$2.4 MILLION

The average cost of

LOST/STOLEN RECORDS

per individual is

$141.00



Damage related to cybercrime is projected to hit

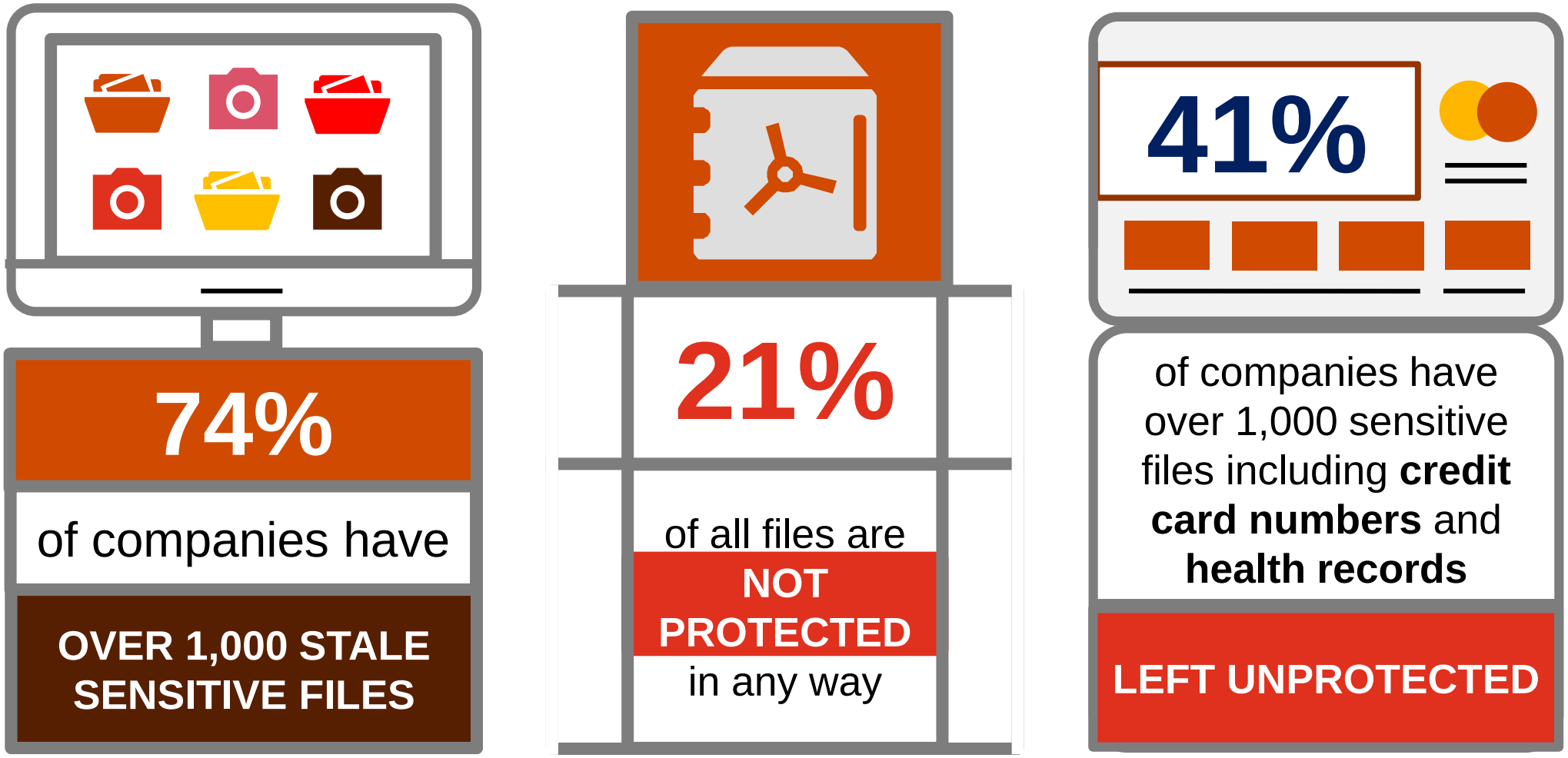
$6

Trillion

ANNUALLY BY 2021

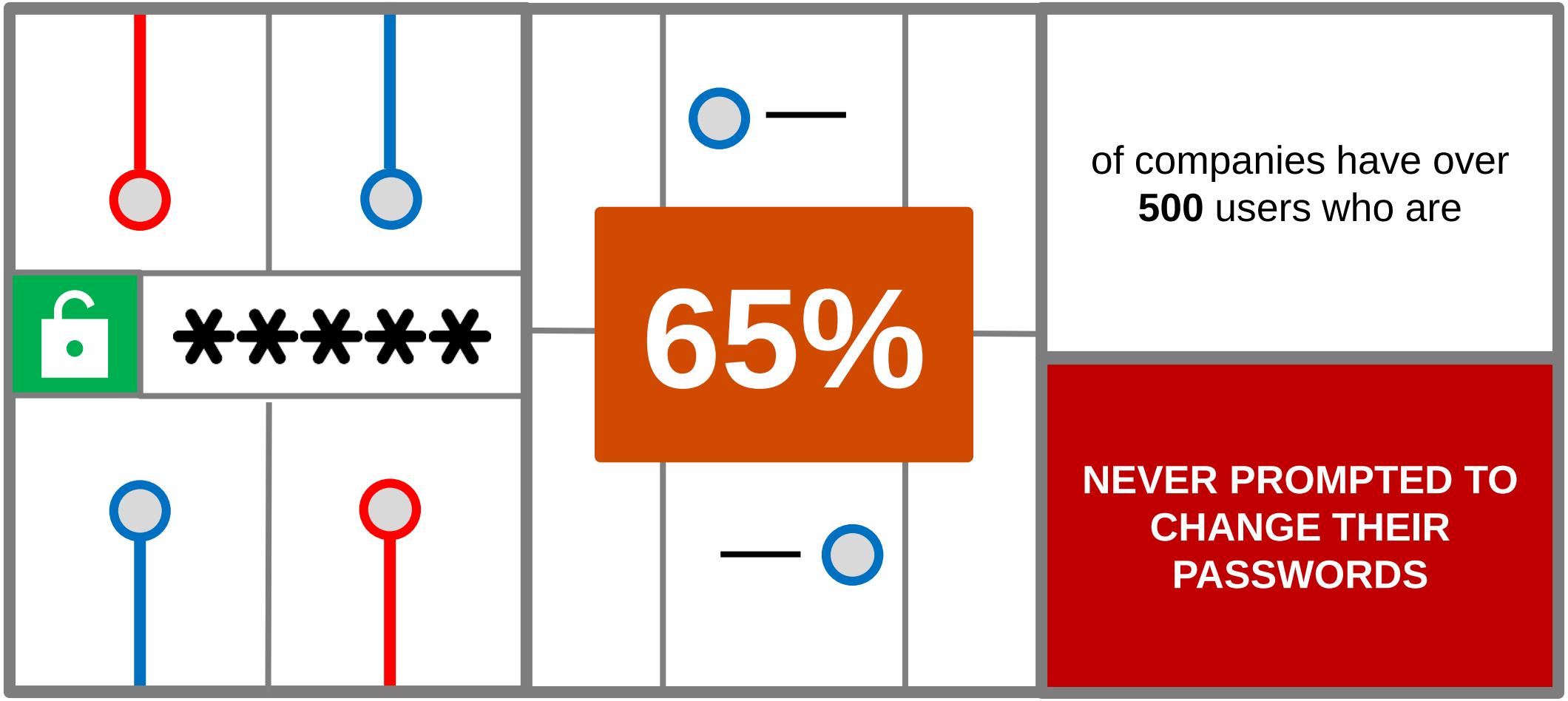
Source: *Facts and figures obtained from varonis.com/blog/cybersecurity-statistics

Is Your Company at Risk?



Source: *Facts and figures obtained from varonis.com/blog/cybersecurity-statistics

Is Your Company at Risk?



Source: *Facts and figures obtained from varonis.com/blog/cybersecurity-statistics

Data security threats

A short video…

Data security threat

E-mail Security

Email is the biggest security threat for most companies.

According to Digital Guardian, 91% of cyber attacks start with a phishing email, making it the number one threat to your business.

91%

Data security threat

Recognizing Social Engineering

1 Playing with your emotions

Phishing emails and malicious websites often dangle a financial reward, or threaten negative consequences, often with a fast-approaching deadline. If something that seems too good to be true, it probably is.

2 Bad Grammar

Poorly constructed sentences, spelling mistakes, and an unusual tone are all signs that an email isn't from who you think it is.

3 Embedded links

Roll your mouse pointer over the link without clicking and check out the web address that appears before you click it.

4 Strange senders

Hover your mouse pointer over the email sender's name to double check the sender's email address

5 Suspicious attachments

Take care when an attachment comes from someone you don't know, weren't expecting the file, or if posted on a questionable website. Take particular care with file types .exe, .zip, .docm, .bat and .xlsm.

Data security threat

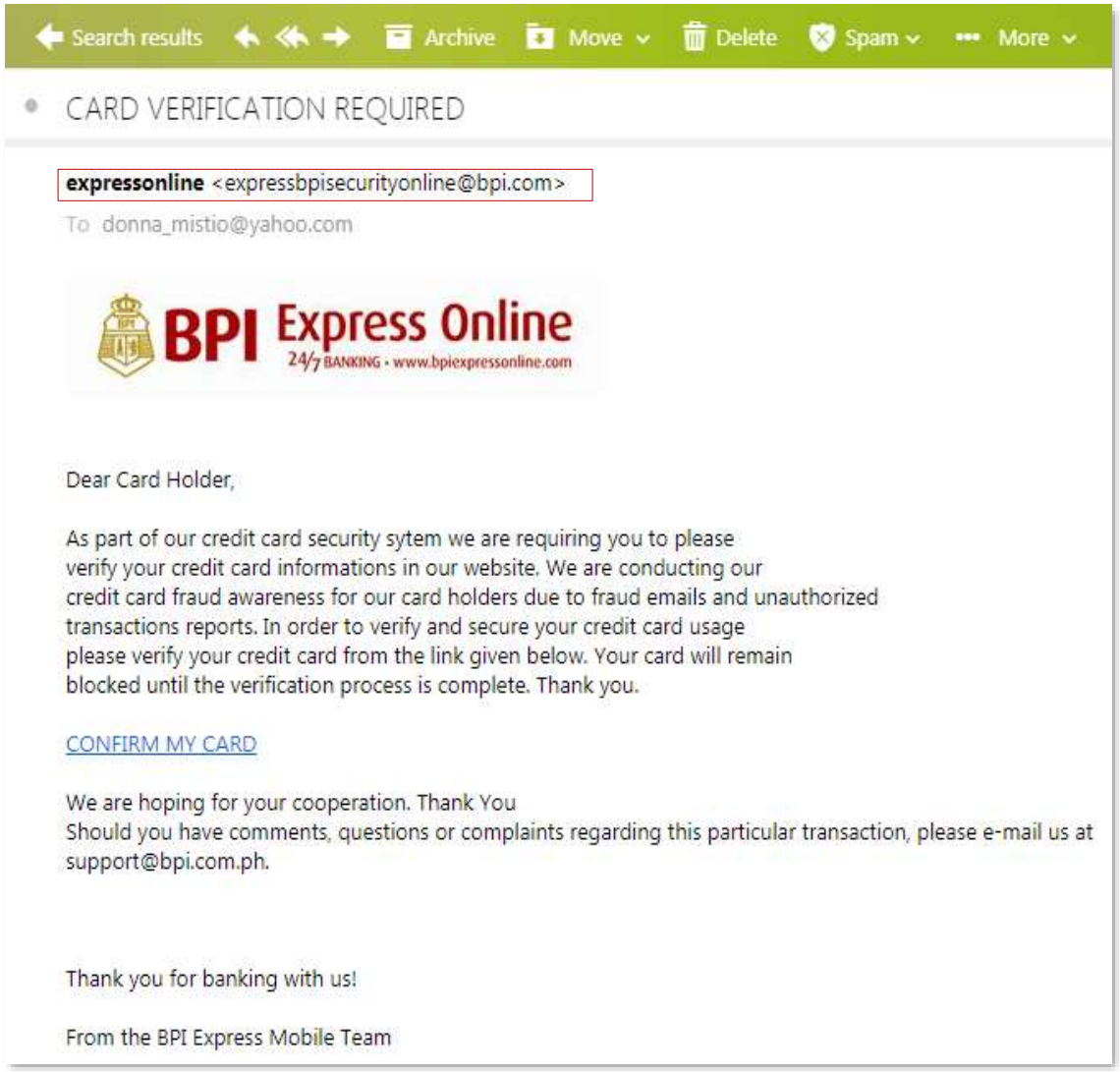
Recognizing Social Engineering

6 Getting personal

On email, genuine companies won't ask for personal details such as your bank accounts, password or PIN via email. If in doubt, contact the organization directly.

7 Payment diversion fraud

When an email or website invites you to re-route company payments, or to set up unexpected new payments, always double check.



Data security threat

If anyone asks for confidential information, ALWAYS be suspicious. If they're a malicious person and get the information they need, the company could be at serious risk.

- Never disclose confidential information to an unknown source, or give out more information than seems necessary
- Don't be afraid to ask questions or ask for ID if you have suspicions
- Watch out for people looking over your shoulder at information on your screen or desk
- If you're suspicious, consult concerned department or personnel before providing information.

Data security threat

Key findings from The Global State of Information Security Survey 2018

28%

Cite mobile device exploitation as the cause of the security incident overtaking phishing attacks as the top threat vector

Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2018, October 18, 2017

Business leaders understand new risks tied to emerging technologies

A short video…

3

Role of CPAs in Mitigating Cyber Attacks

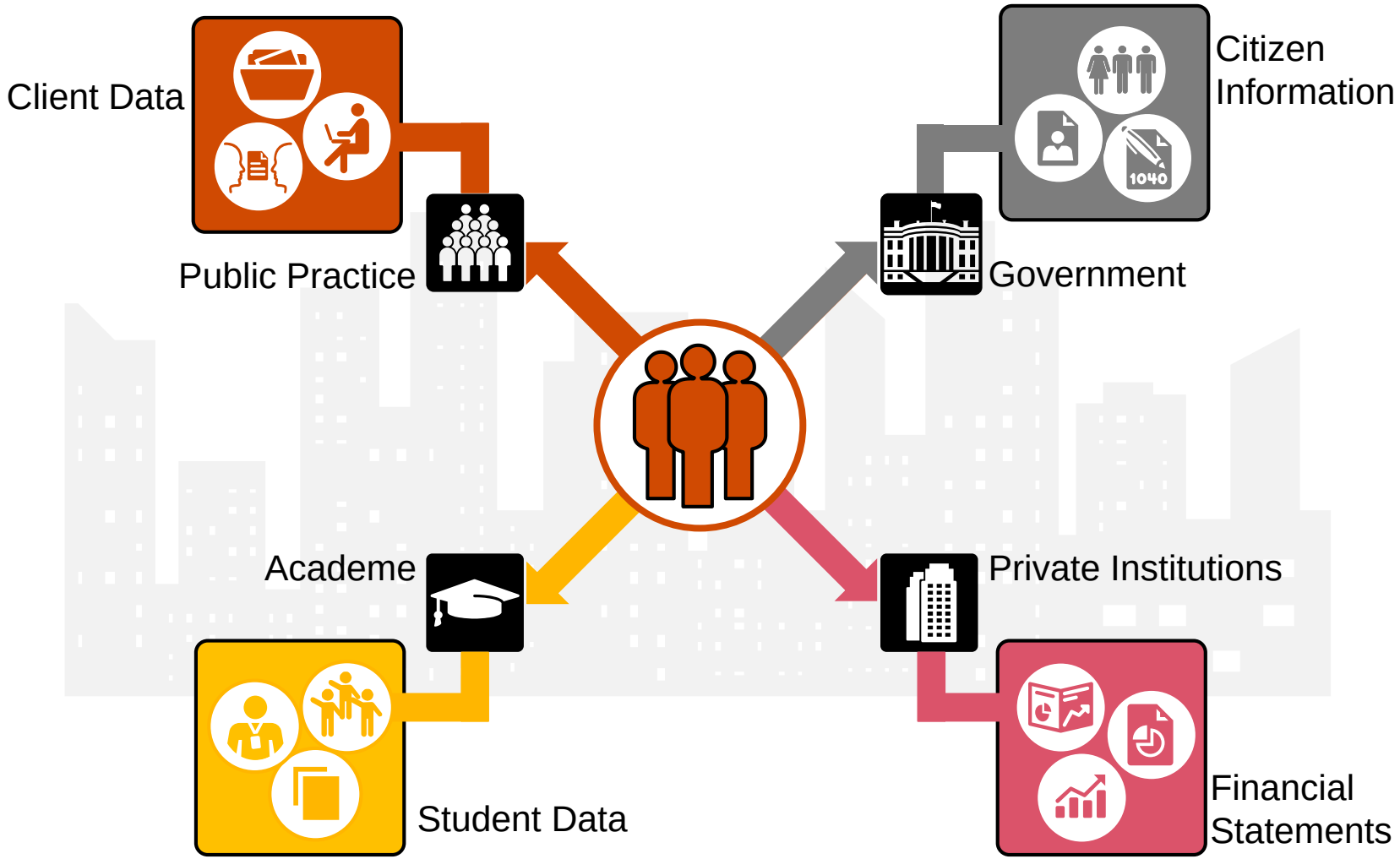
“

Accountants and other financial institutions are particularly attractive to cyber criminals. In fact, PwC estimate that financial institutions are over 30% more likely to be targeted than other companies.

Association of Chartered Certified Accountants (ACCA) Global
https://www.accaglobal.com/ie/en/student/sa/features/cyber.html

The CPAs role in maintaining security and promoting data privacy
Isla Lipana & Co., PwC

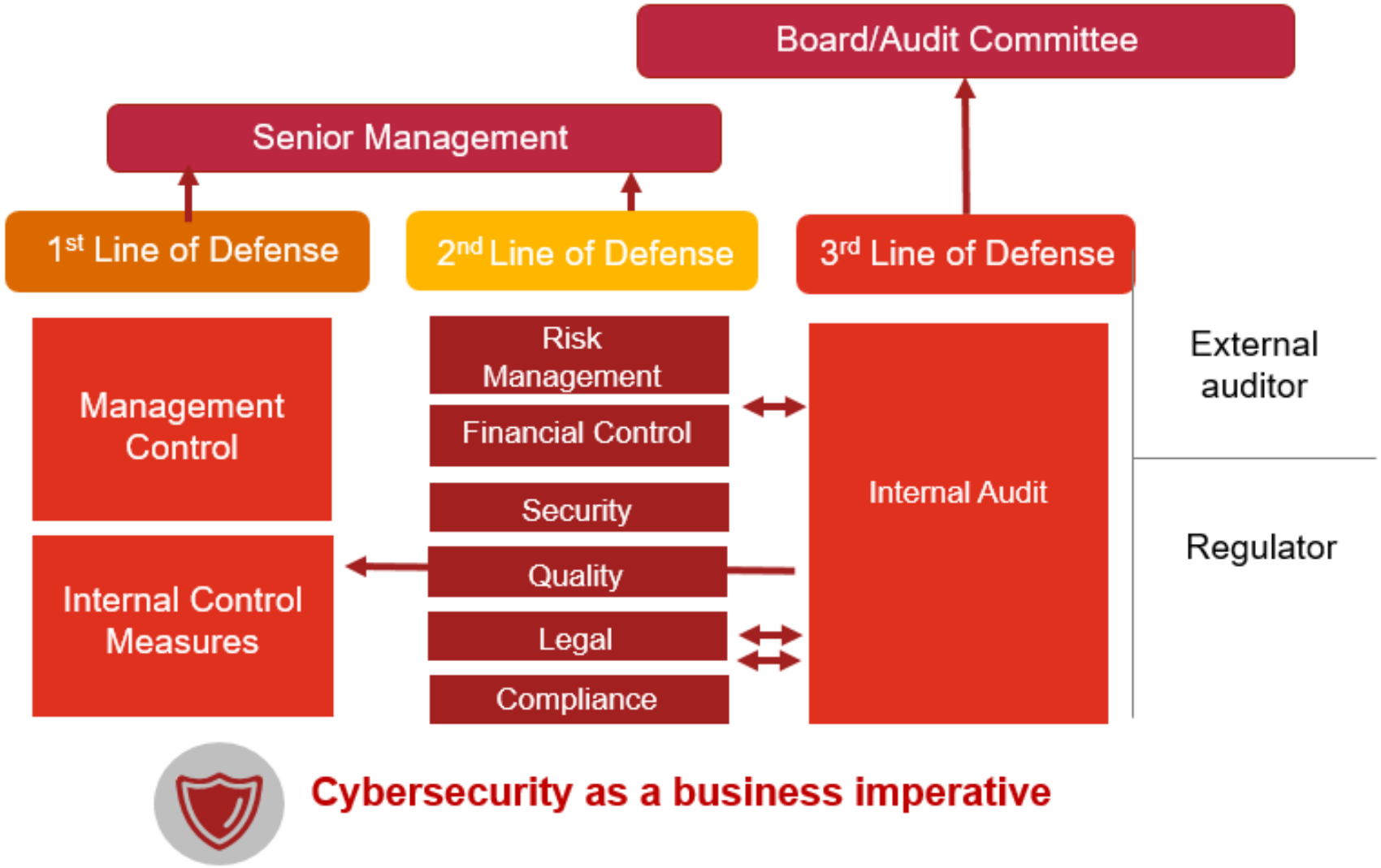
Sectors and Data Related to Accountants



The “Three Lines of Defense”

Who is responsible for security?

In 2012, IIA introduced the concept of three lines of defense to help organizations manage business risk. Widely differing opinions about who plays what role in which process.



The “Three Lines of Defense”

Responsible for the RISK and CONTROL Area

Manages the day-to-day execution and management of risks and controls

- Assigning risk and control owners
- Identification and evaluation of risks by risk owners
- Execution of controls by control owners
- Risk enabled decision making
- Addressing gaps by implementing controls to mitigate risks and keep them at the desired level
- Reporting relevant information to relevant stakeholders

Reinforce first line of defense’ ownership of cyber and privacy risk by the business

The “Three Lines of Defense”

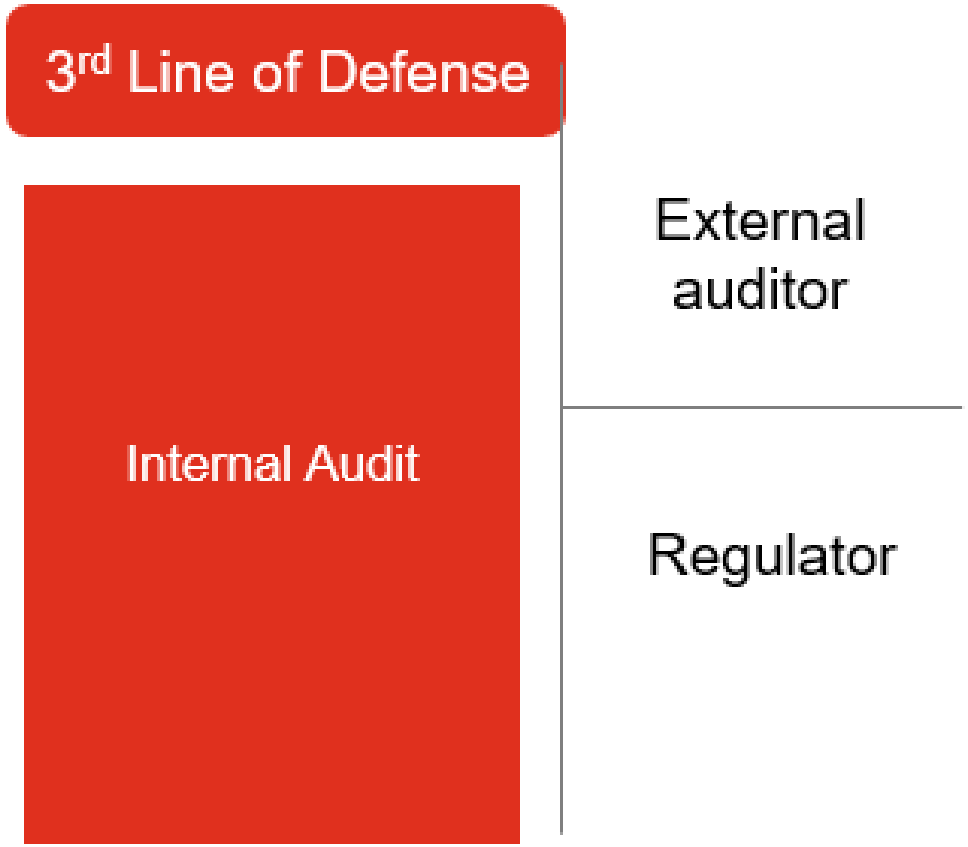
It has oversight responsibilities.

Responsibilities:

- Prepare risk assessments
- Perform testing
- Monitor how management addresses identified issues and findings.
- May own certain compliance risk management initiatives and controls such as anti-bribery, conflicts of interest or privacy.

Build an effective second line of defense model for cyber and data privacy risk management

The “Three Lines of Defense”



Responsible for reviewing that a company’s **risks are being managed** through the assessment of its internal control framework.

‘The Independent Assurance’

Successful “Three Lines of Defense”

The cornerstone of a successful three lines of defense model is the ability of the organization to create a central foundation

- Common definitions and processes
- Clear delineation of roles and responsibilities
- Efficient collaboration and information sharing across all parties

Considerations to achieve data security

Areas of Focus

Considerations to achieve data security

Areas of Focus

1 Accountability: Own the risk

- ❑ Data security risk is owned by leadership and is not relegated to the IT function.
- ❑ Periodic information security briefings are provided to the Board and C-Suite.

Considerations to achieve data security

Areas of Focus

1. Accountability: Own the risk
2. Priority: You cannot secure everything

- ❑ Leadership prioritizes and monitors information security investments.
- ❑ Crown jewels have been identified and their protection prioritized.
- ❑ Investments are made in new capability, not just technology.

Considerations to achieve data security

Areas of Focus

1. Accountability: Own the risk
2. Priority: You cannot secure everything
3. Connections: Their risk is your risk

- ❑ Security of the business value chain including suppliers, third party providers and high-risk interconnection points has been considered.
- ❑ Adapt to the challenges of new and emerging digital business models.

Considerations to achieve data security

Areas of Focus

1. Accountability: Own the risk
2. Priority: You cannot secure everything
3. Connections: Their risk is your risk
4. People: People do matter

- ❑ A security culture and mindset is established through training, measurement and evaluation.
- ❑ Behaviors and capabilities of the organization are established and reinforce the importance of data security.

Considerations to achieve data security

Areas of Focus

1. Accountability: Own the risk
2. Priority: You cannot secure everything
3. Connections: Their risk is your risk
4. People: People do matter
5. Technology: Fix the basics

- ❑ Maintain a good IT security hygiene
- ❑ Identify and effectively manage data access
- ❑ Employ security intelligence and analytics

Considerations to achieve data security

Areas of Focus

1. Accountability: Own the risk
2. Priority: You cannot secure everything
3. Connections: Their risk is your risk
4. People: People do matter
5. Technology: Fix the basics
6. Crisis: It's not if, but when

- ❑ Implement continuous monitoring and detection
- ❑ Establish and test your crisis management plan

4

Tips to Protect Oneself from Cyber Threats

A short video…

> Accountants are well placed to advise on the steps a business should take to protect itself – data security isn't just about technology and computers: it involves people, information, systems, processes and culture too.

John Berriman, Former Board Member and CFO of PwC UK

5

Q&A

Thank you

pwc.com/ph