MCUL CUsolutions GROUP
MICHIGAN CREDIT UNION LEAGUE & AFFILIATES

Securing Your Information Assets

Presented by Scott Petree and Andrea Selke

June 10, 2016 | 2:15 pm

Visit www.mculace.com to Access Handouts From Select Sessions

plante moran
audit • tax • consulting

Todays Presenters

Scott Petree CPA, CISA, CFE, QSA

Principal, Cybersecurity

Andrea Selke CISSP

Manager, Cybersecurity

plante moran
audit • tax • consulting

Agenda

Pop Quiz!

Current Trends in Security

What does a hack look like?

How does this end?

plante moran

audit • tax • consulting

Pop Quiz!

plante moran
audit • tax • consulting

Pop Quiz

{Cost of a breach?}

What is the cost per record of a data breach?

A. 201 Dollars

B. 58 Cents

C. 9 Cents

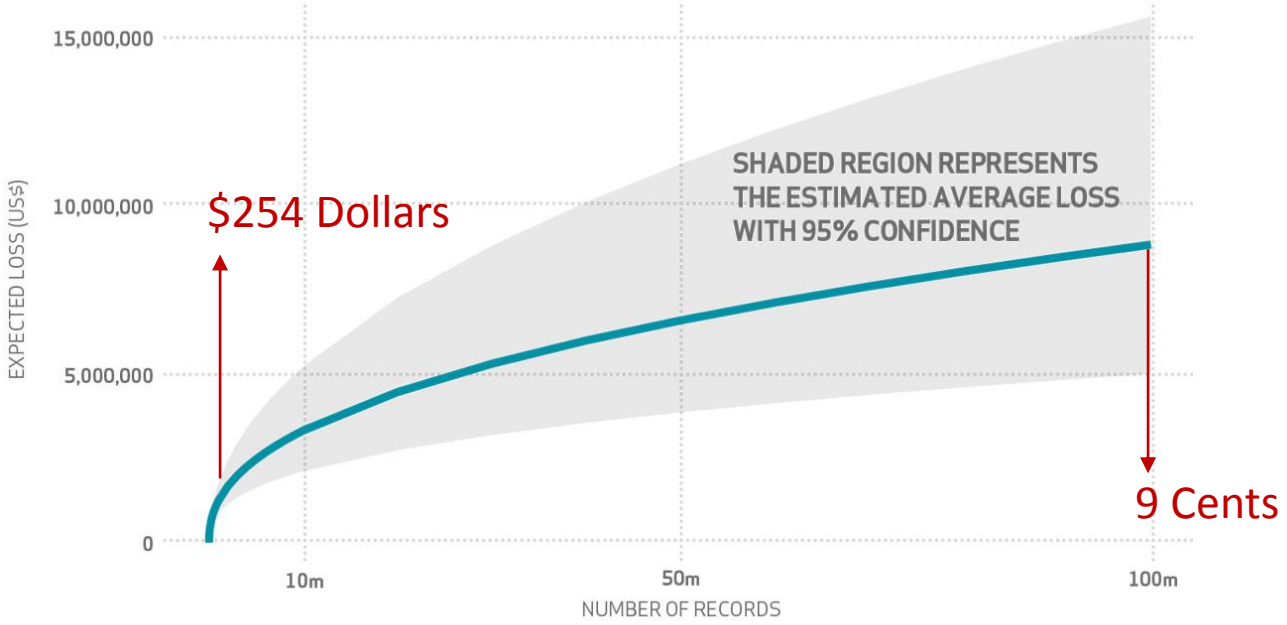
plante moran
audit • tax • consulting

Pop Quiz

{Cost of a breach?}

All of the Above!

(could be anywhere from 9 cents to $254 depending on the number of records lost)



Source: 2015 Verizon Data Breach Report

plante moran
audit • tax • consulting

Pop Quiz

{Cost of a breach?}

The overall average cost of data breach is currently…

$3.8 million

The total average cost of a data breach is now $3.8 million, up from $3.5 million a year ago, according to a 2015 study by data security research organization Ponemon Institute

plante moran
audit • tax • consulting

Pop Quiz

{Cost of a breach?}

The selling price of basic member records is currently:

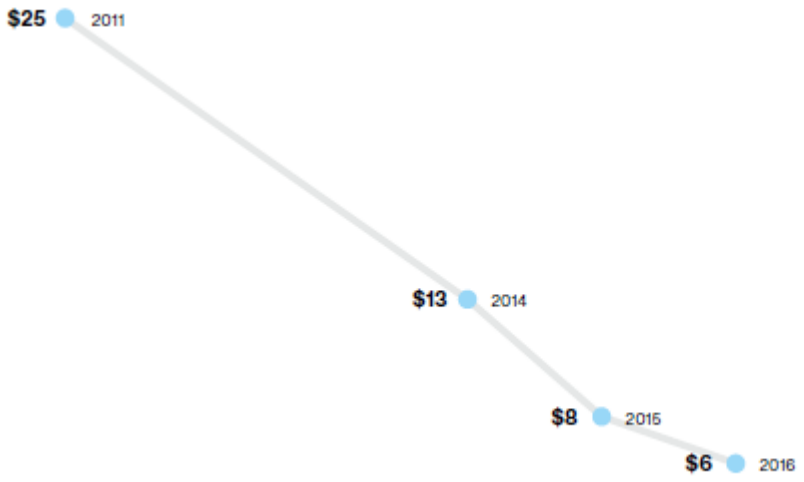


Figure 47.
Price per payment card record over time (USD). Source: Intel Security

With supply through the roof, prices have lowered for member records; driving the market to now charge extra for valuable services such as selling by geographic location, adding SSN's, or additional upcharges.

Source: 2016 Verizon Data Breach Report

plante moran
audit • tax • consulting

Pop Quiz

{Speed of a breach?}

How long does it take an attacker to compromise your systems?

A. Seconds
B. Minutes
C. Hours
D. Days

plante moran
audit • tax • consulting

Pop Quiz

{Speed of a breach?}

A/B: Seconds/Minutes

in 11% of cases, it took attackers just seconds to compromise systems

in 82% of cases, attackers were in within minutes

Source: 2016 Verizon Data Breach Report

plante moran
audit • tax • consulting

Pop Quiz

{Your data went where?}

How long does it take an attacker to exfiltrate data?

A. Minutes
B. Days
C. Weeks

plante moran
audit • tax • consulting

Pop Quiz

{Your data went where?}

A: Minutes

(in 21% of cases, it took attackers just minutes to exfiltrate data)

Source: 2016 Verizon Data Breach Report

plante moran
audit • tax • consulting

Pop Quiz

{Speed of breach detection?}

How long does it take to find out that there's been a breach?

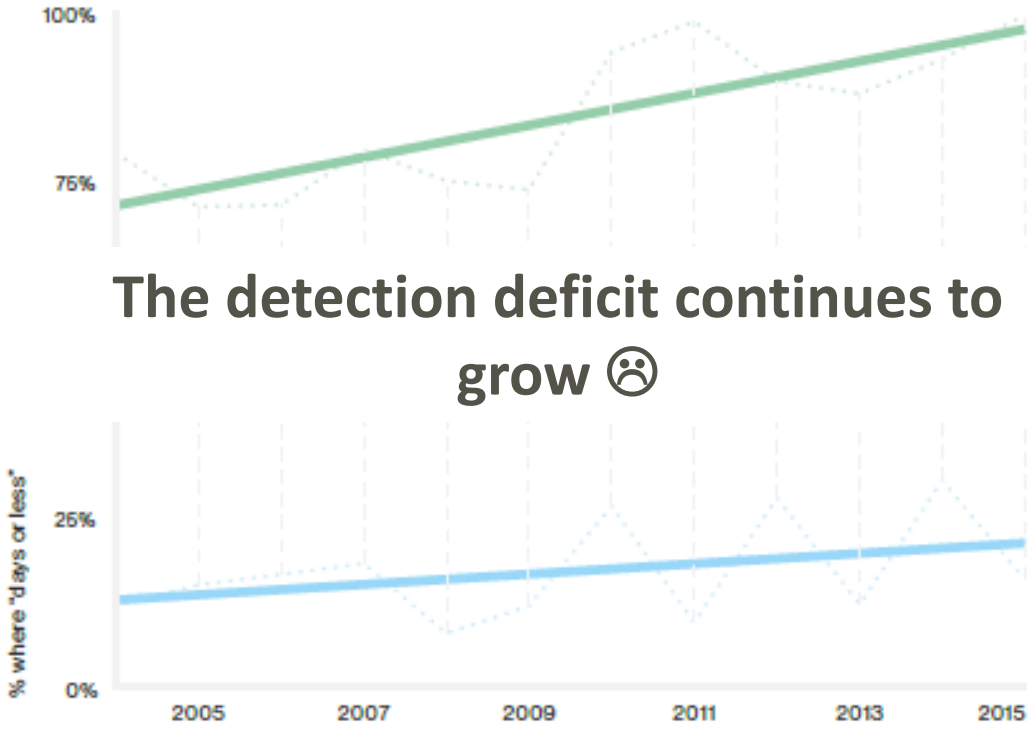
A. Minutes
B. Days
C. Weeks

plante moran
audit • tax • consulting

Pop Quiz

{Speed of breach detection?}

B and C: Days, Weeks and **sometimes months**!



The detection deficit continues to grow ☹

Figure 8.

Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less

Source: 2016 Verizon Data Breach Report

plante moran
audit • tax • consulting

Pop Quiz

{Volume of breaches?}

How many financial institutions had a confirmed data loss in 2015?

A. <10 monthly
B. 10-50 monthly
C. >50 monthly

plante moran
audit • tax • consulting

Pop Quiz

{Volume of breaches?}

C. >50 monthly

795 confirmed breaches in 2015, or over 66 on average monthly

Source: 2016 Verizon Data Breach Report

plante moran
audit • tax • consulting

Pop Quiz

{How old was that hack?}

What was the most common age of vulnerabilities seen last year?

A. Eight years old
B. Three years old
C. Less than a year old

plante moran
audit • tax • consulting

Pop Quiz

{How old was that hack?}

A: In 2016, Verizon found more vulnerabilities dating back to 2007 than from any year between 1999 and 2016

(Believe it or not, some hackers are still partying like it's 1999!)

85% of successful exploited traffic relate to the top 10 vulnerabilities

Source: 2016 Verizon Data Breach Report

plante moran

audit • tax • consulting

Trends in Information Security

plante moran
audit • tax • consulting

Trends in Information Security

{Who are the victims?}

Targets — victims of opportunity:

Some will be **a target** regardless of what they do, but most become a target **because of what they don't do** related to security.

plante moran
audit • tax • consulting

Trends in Information Security

{How are they hacking us?}

Most common attack — social:

Most attacks began socially. Employees are your greatest asset, but often your weakest link to security.

Hackers know this, and have developed social scams by the thousands, hoping but one will fall victim.

23%
OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

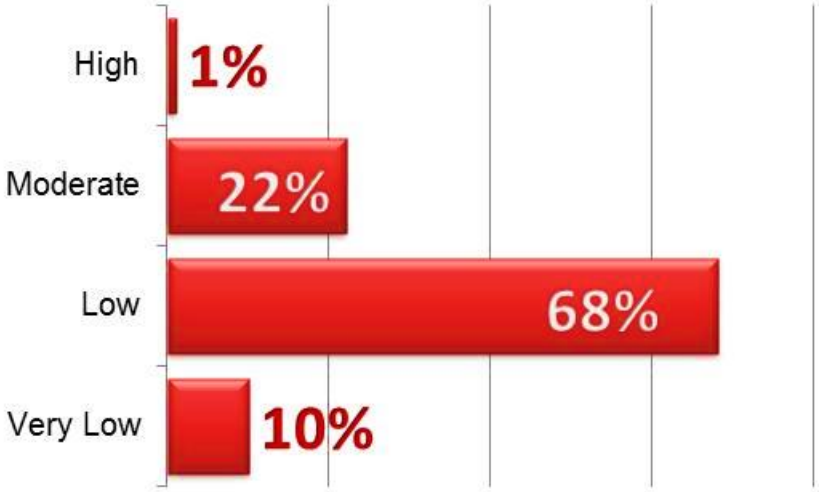
plante moran
audit • tax • consulting

Trends in Information Security

{Could this be prevented?}

Prevention — not rocket science:

Most victims weren't overpowered by unknowable and unstoppable attacks. We know them well enough and we also know how to stop them.



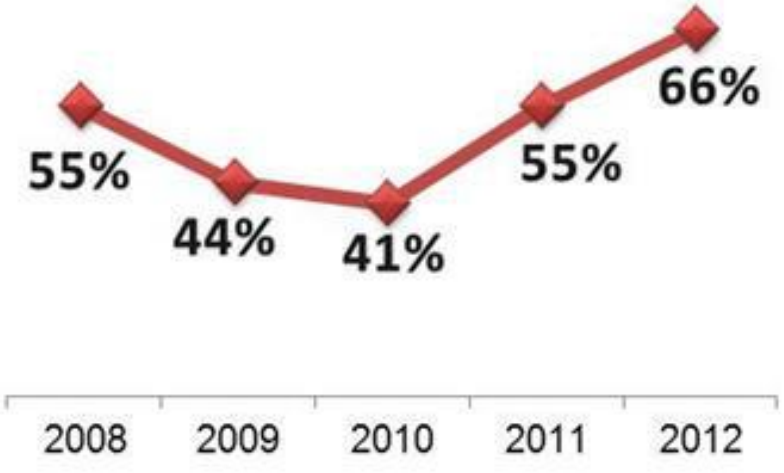
plante moran
audit • tax • consulting

Trends in Information Security

{Why can't we stop them?}

Breaches in 2014 — went unnoticed:

Prevention is crucial, but we must accept the fact that no barrier is impenetrable. Detection/response represents an extremely critical defense.



70–90%
OF MALWARE SAMPLES ARE UNIQUE TO AN ORGANIZATION.

plante moran

audit • tax • consulting

What does a hack look like?

plante moran
audit • tax • consulting

What does a hack look like?

{Example attack… LIVE!!!}

plante moran
audit • tax • consulting

Hackers – What do they want?

{Sony & others prove - anything and everything!}

- Personally identifiable information
- Credit Card Data
- Usernames & Passwords
- E-mail
- Trade Secrets
- Customer Lists
- Vendor Lists
- COULD BE ANYTHING!

97% of breaches were avoidable

Most victims aren't overpowered by unknowable and unstoppable attacks. For the most part, we know them well enough and we also know how to stop them

Verizon Data Breach Investigations Report

User Ignorance

Weak user passwords
Poor judgment
Social media
Phishing attacks

Weak infrastructure

Weak design (firewalls, wireless routers)
Weak user authentication (users, passwords)
Encryption (VPN, secure portals)
Out-dated (patch management / anti-virus)
Lack of periodic testing

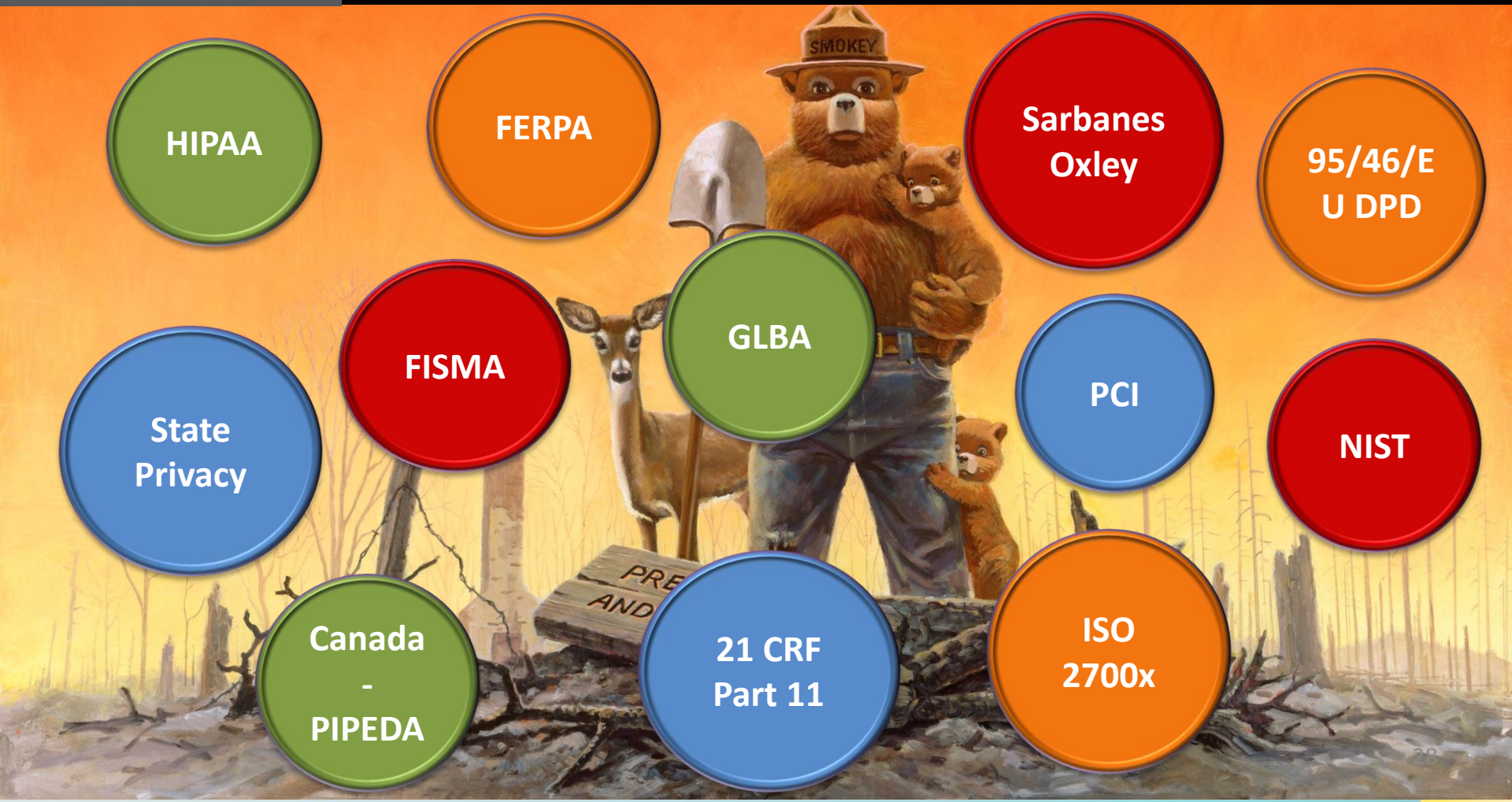
Technology Advances

Mobile devices
Cloud computing / public portals

plante moran
audit • tax • consulting

Breaches – Can they be stopped?

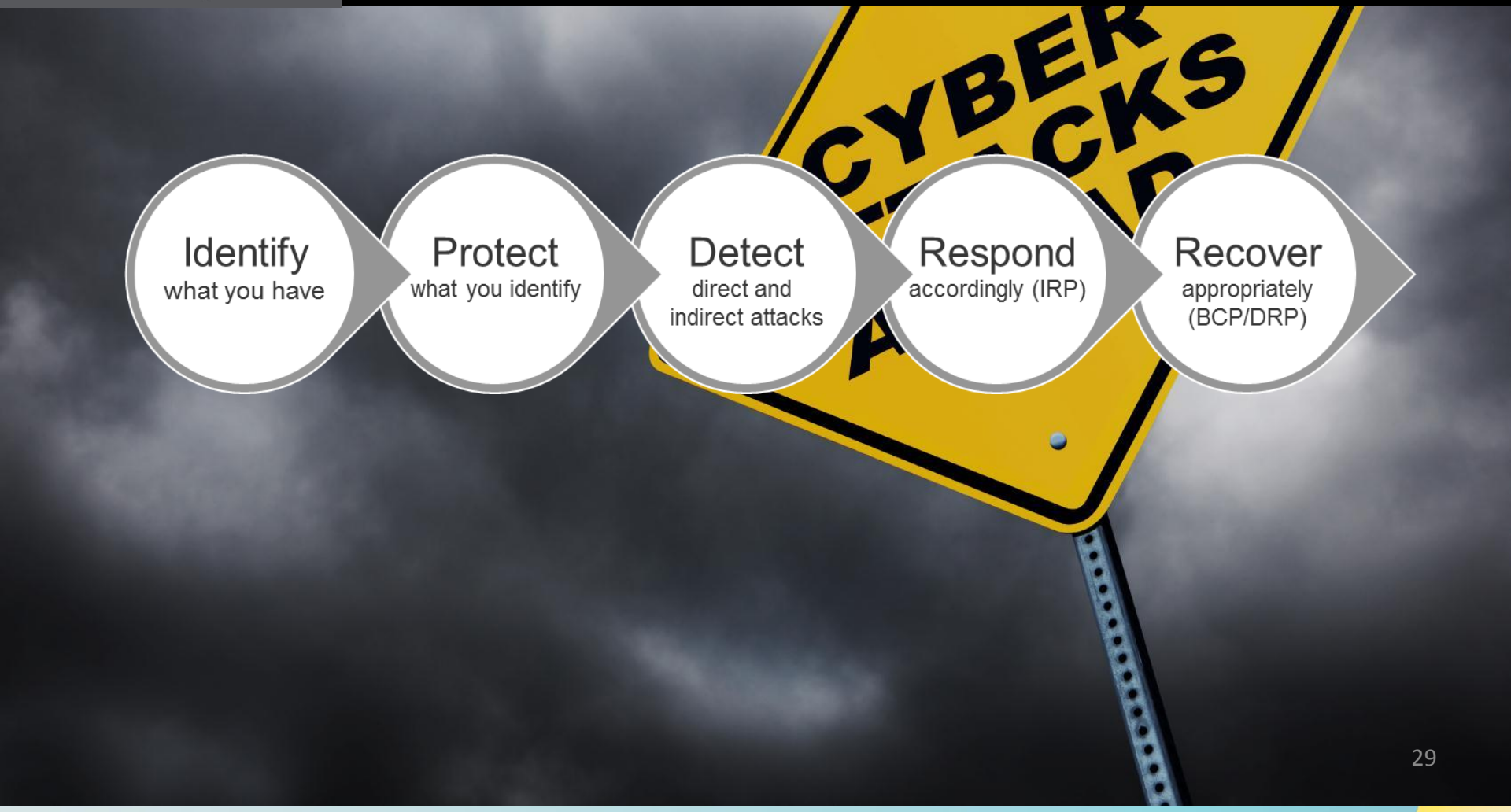
{Don't count on Regulation or Standards!}



plante moran
audit • tax • consulting

Breaches – Can they be stopped?

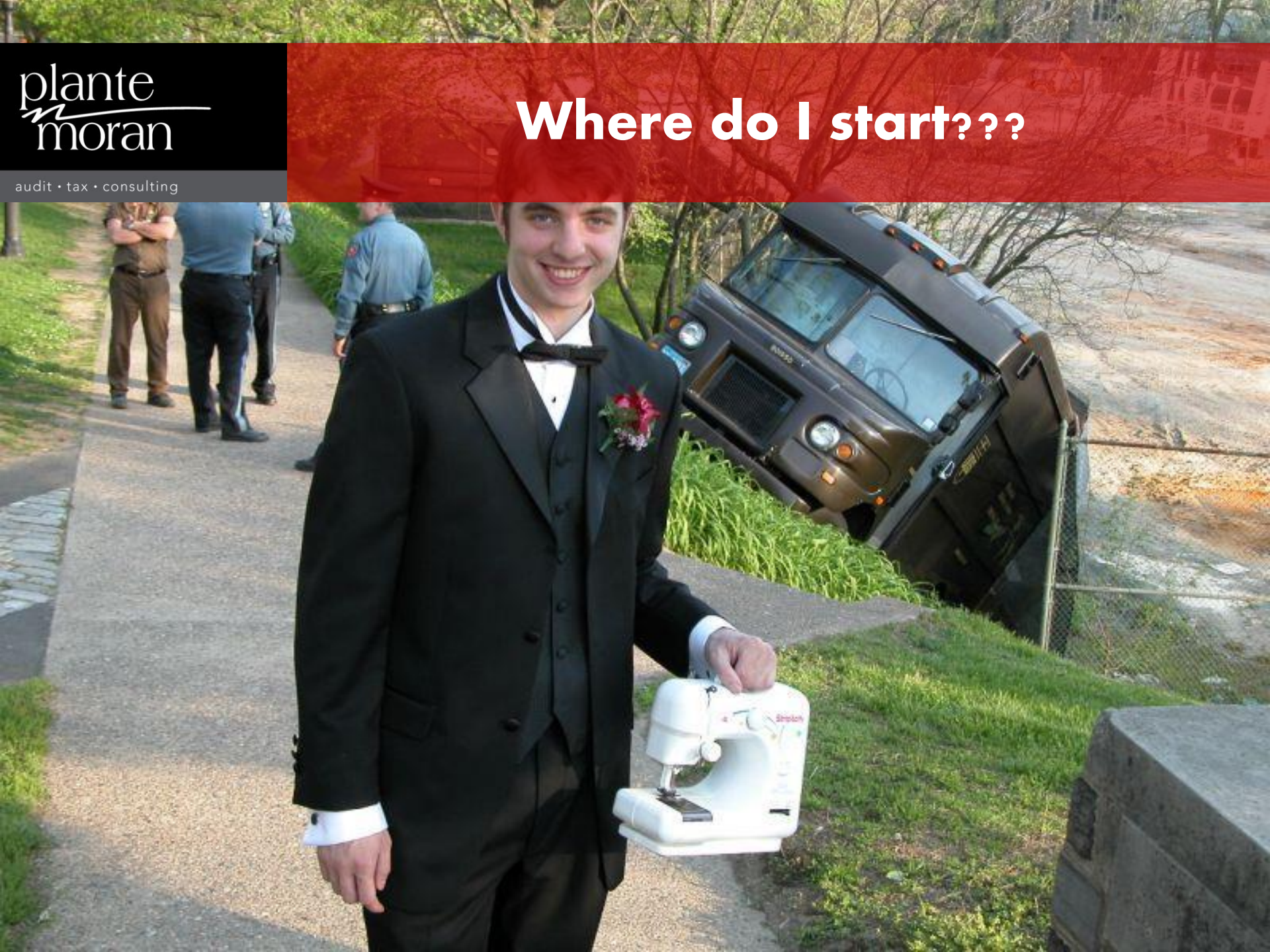
{But don't ignore them either!!}



plante moran

audit • tax • consulting

Where do I start???

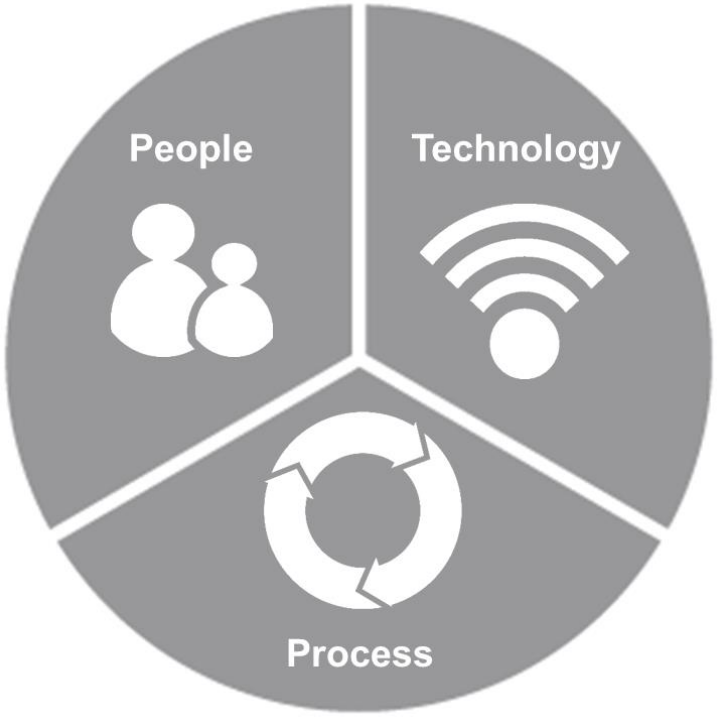


plante moran
audit • tax • consulting

Where do I start?

{Start with a realization!}

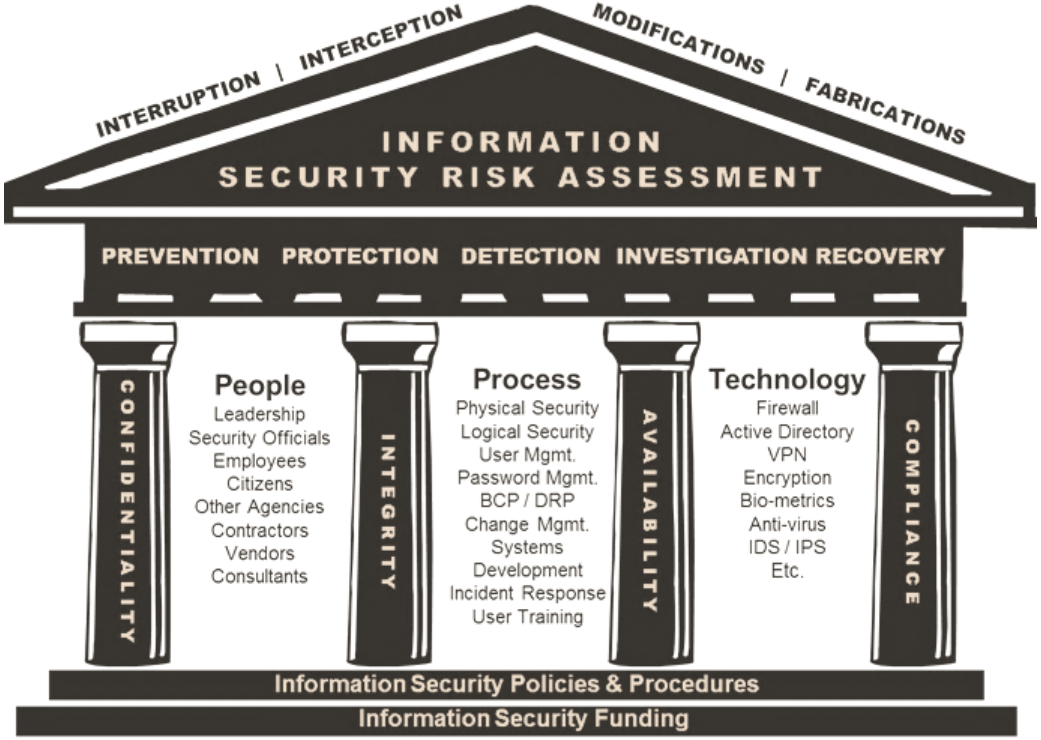
Realize that Information Security is NOT an IT issue: it is a Business issue.



plante moran
audit • tax • consulting

Where do I start?

{Act on that realization!}



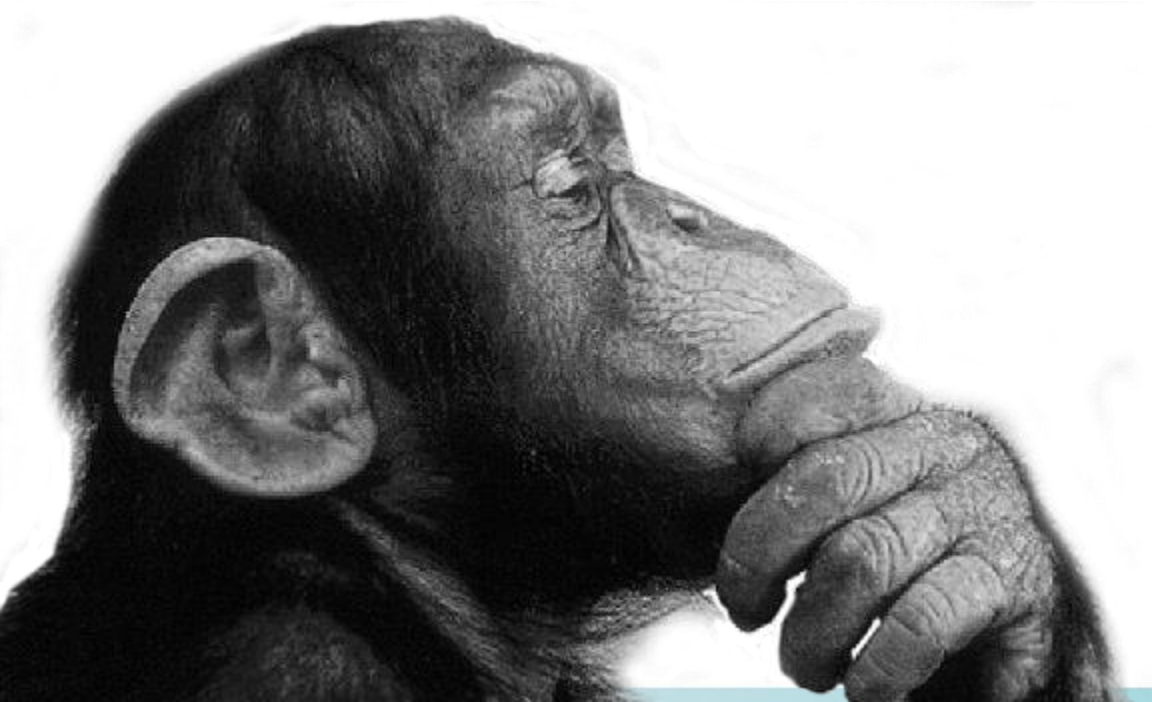
Different organizations view information security differently. Some of the differences are related to varied risk and threat profiles impacting an organization — based on factors such as industry, location, products/services, etc. Other differences are related to management's view of security based on their experience with prior security incidents.

plante moran
audit • tax • consulting

Who is ultimately responsible?

{you are!}

You don't have to be a security professional to think critically!

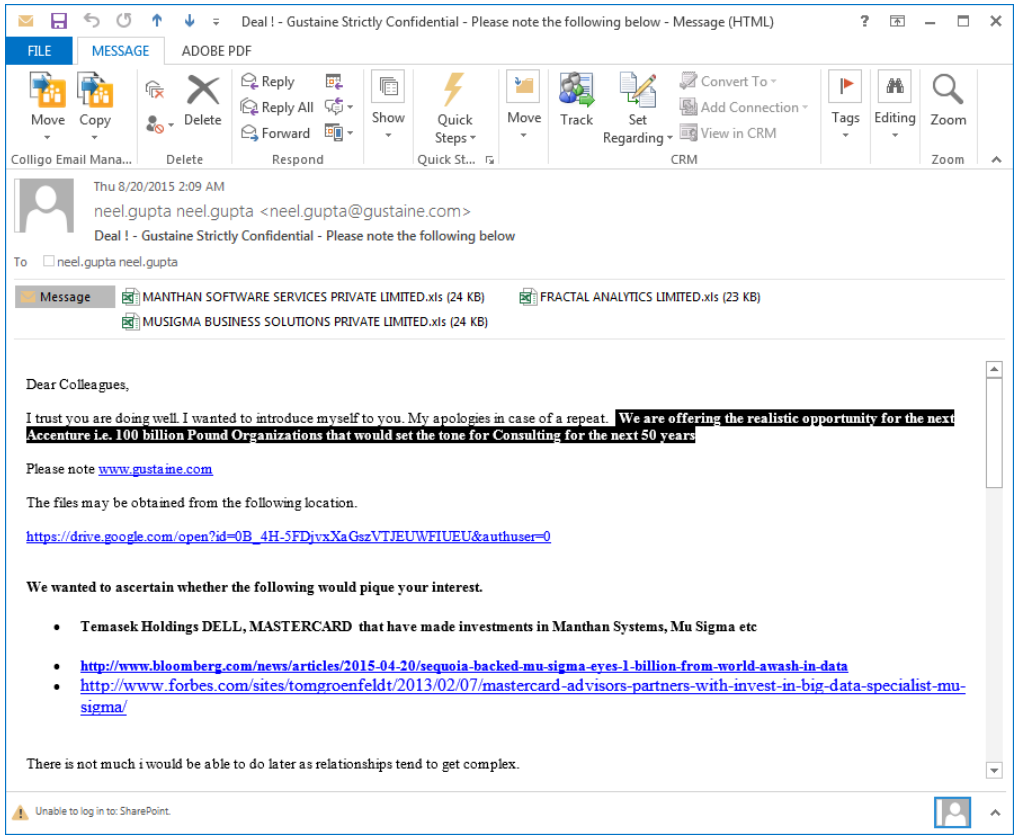


plante moran
audit • tax • consulting

Who is ultimately responsible?

{you are!}

You don't know a Nigerian Prince, you didn't win the Malaysian Lottery, and you don't have the investment opportunity of a lifetime:

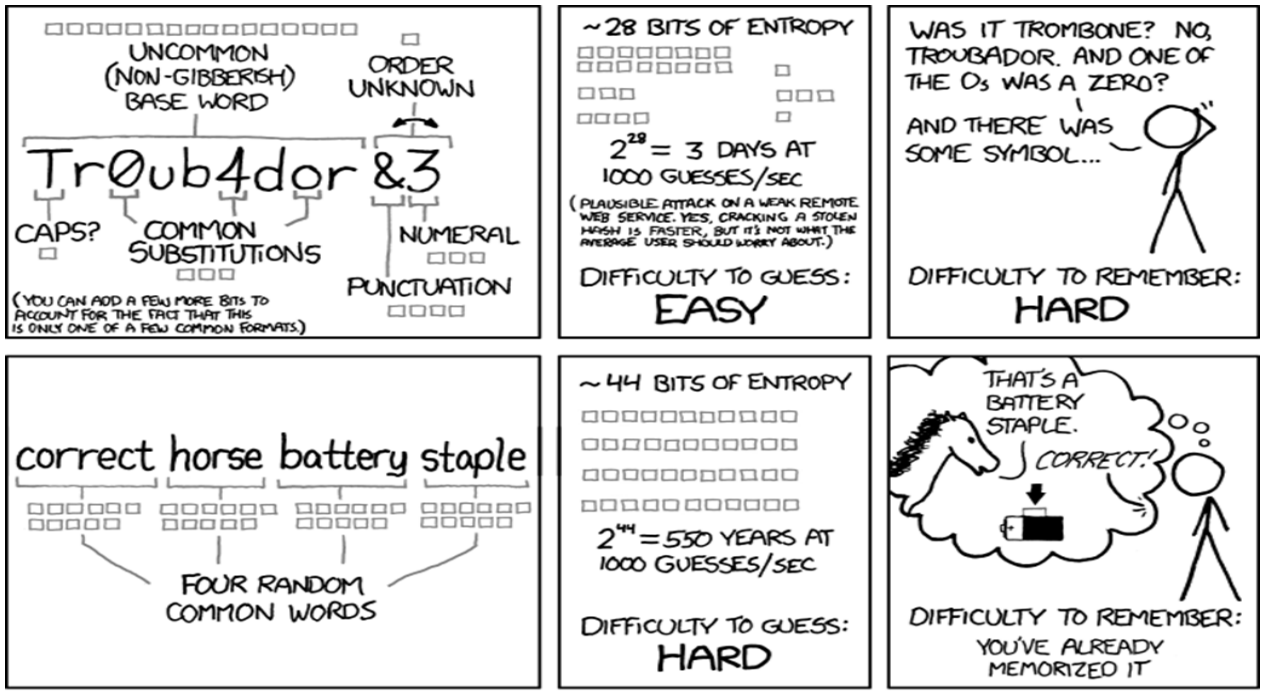


plante moran
audit • tax • consulting

Who is ultimately responsible?

{you are!}

Don't use a password!



plante moran
audit • tax • consulting

How does this end?

{It doesn't!}

Realize that Information Security does not end. It can only be maintained through constant vigilance, training, and reassessment.

plante moran

audit • tax • consulting

THANK YOU

QUESTIONS? PLEASE CONTACT

SCOTT PETREE | PRINCIPAL | CYBERSECURITY

248.223.3898 | SCOTT.PETREE@PLANTEMORAN.COM

ANDREA SELKE | MANAGER | CYBERSECURITY

248.223.3224 | ANDREA.SELKE@PLANTEMORAN.COM