SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

Secure your business against Cybercrime

Presenter: Ferdie van Schalkwyk - IPMG

Understand the basics of Cybersecurity in business terms

SA | ACCOUNTING ACADEMY

Connect. Partner. Succeed.

About SAAA

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

Creating opportunities to connect our partners to succeed

SAAA offers CPD training for accountants, auditors, bookkeepers and tax practitioners. We give you access to professional and technical content that ensures both your knowledge and skills are maintained so you remain professionally competent.

The CPD policy is compliant with IFAC IES7

All training offered by SAAA is recognised for CPD hours by the relevant professional bodies.

SAAA Rewards

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

CPD Subscribers gain access to various rewards

These can be accessed from your profile by logging in and navigating to your “My Rewards” > “Find out more” to see the reward partner benefits and claim it.

These rewards include discounts, reduced premiums and free stuff.

Reward Partners

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

ACTS ONLINE

Acts Online provides legislation, including amendments and regulations, in an intuitive, online format.

DRAFTWORX™
Financial Statements | Working Papers

Draftworx provides automated drafting and working paper financial software.

EdNVest

EdNVest offers an exciting and unique product that leverages Section 10(1)(q) of the Income Tax Act

InfoDocs

InfoDocs Company Secretarial Software.

Reward Partners

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

PRACTICE Ignition

Practice Ignition simplifies onboarding - from engagement letter creation to securing client signatures.

intuit quickbooks

QuickBooks Cloud Accounting Platform: The one place to grow and manage your entire practice.

the tax shop ACCOUNTANTS

Join the largest accounting and tax franchise in Southern Africa.

Webinar Housekeeping

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

The webinar recording and presentation will be available at the end of the webinar within your SAAA profile.

These can be accessed from your profile by logging in and navigating to your “My Dashboard” > “View Events” and then clicking on “Links & Resources” next to the webinar title.

The webinar is available under the “Recording(s)” tab and the presentation under the “Files” tab.

Claiming CPD Hours

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

You can claim your CPD hours for this webinar at the end of the webinar within your SAAA profile.

This can be accessed from your profile by logging in and navigating to your “My Dashboard” > “View Events” and then clicking on “Links & Resources” next to the webinar title.

The “Claim My CPD” option is available under the “CPD” tab. Once claimed you will be able to view and download your certificate.

Disclaimer

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

Disclaimer

Whilst every effort has been made to ensure the accuracy of this presentation and handouts, the presenters / authors, the organisers do not accept any responsibility for any opinions expressed by the presenters / author, contributors or correspondents, nor for the accuracy of any information contained in the handouts.

Copyright

Ask Questions

SA | ACCOUNTING ACADEMY
Connect. Partner. Succeed

To ask questions and interact during the webinar please use the chat sidebar to the right of the video / presentation on the screen.

Feel free to ask your questions during the webinar in the chat, these will be address in the formal Q & A at the end of the presentation.

Secure your business against Cybercrime

IPMG IT and Business Solutions is an independent firm of consultants focused on providing business solutions to our SME and corporate clients.

IPMG

Agenda

1. Webinar Topic (90min)
2. Questions and Answers (30min)

IPMG

Why IPMG IT and Business Solutions?

IPMG IT and Business Solutions is an independent firm of consultants focused on providing business solutions to our SME and corporate clients.

IPMG CONSULTING RESOURCES

Ferdie van Schalkwyk

- IPMG IT and Business Solutions
- Focus Areas
  - Technology Consulting and Strategy (I&T)
  - Business Systems Analyst
  - Systems Consultant

Gary Geddis

- IPMG Group CEO
- Focus Areas
  - Strategic Partnerships
  - Governance Consulting (GRC)
  - Organisational Risk Management

Extended Consulting Team

Pierre Norden

- Business Systems Analyst
- Systems Consultant

Marinda Steenkamp

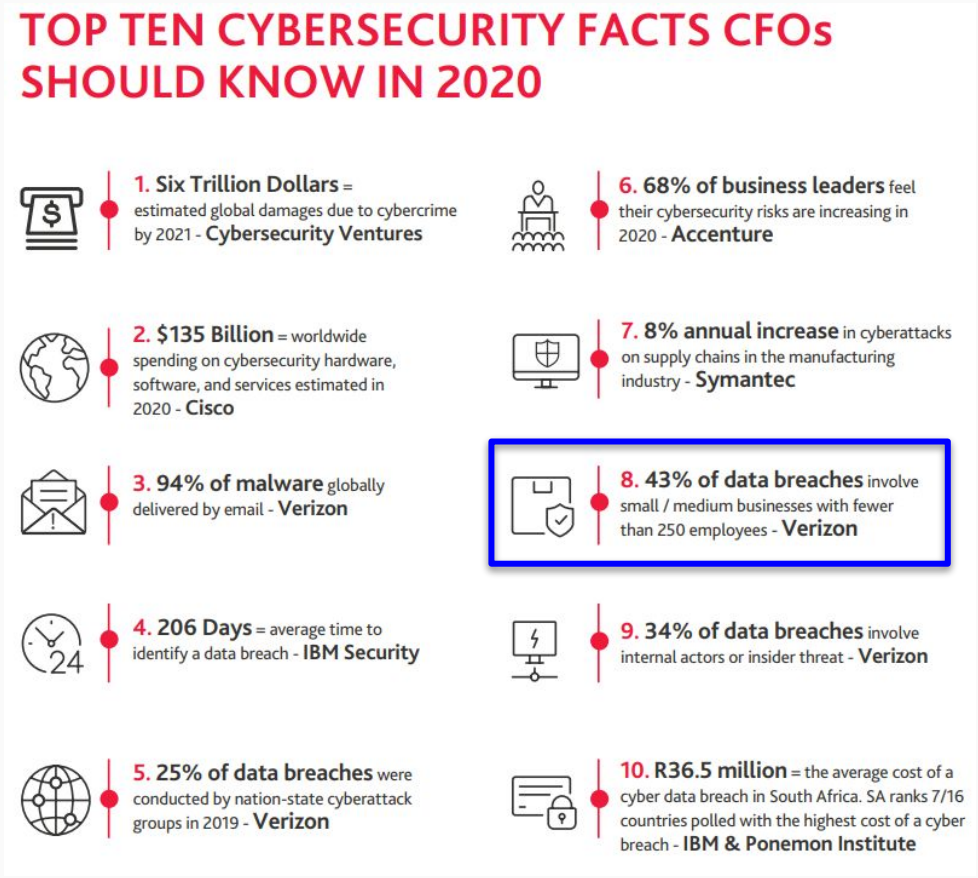
- Business Analyst
- BI Dashboarding

Network Partners

- Business Consultants
- Accounting and Financial Services
- IT Service providers
- Internet Service Providers
- HR, IT Consultants
- Risk Management

Empowering clients to make informed decisions

Background



Small business is a developing the soft target

That is the focus of this Webinar

[Source: BDO newsletter - 4 August 2020]

Target Audience for this Webinar

Most of the advice here is tailored for practices of between 15 and 75 staff

However, for smaller practices, much of the advice is directly transferable or can be easily simplified

For larger practices, the principles will be the same, but the approach more comprehensive.

We assume that you have little to no technology background beyond your day to day interactions with systems as a partner, CA or management responsibilities

Key Objectives

1. Understand the basics of Cybersecurity in business terms
2. Understand the typical weaknesses exploited by Cybercriminals
3. Basic guide for self-assessing and improving your Cybersecurity
    a. Checklist of the non-negotiable and easy wins
    b. The common mistakes
    c. Roles and responsibilities (business and technical)

Scope

- Understand the motive of Cybercriminals
  - How do they make money
  - How do they select targets
- Case Studies - Real word cases
  - How did they get in
  - What was the response
  - What was the outcome
  - How should it have been prevented
- Cybersecurity in your firm
  - What are your duty of care and legislative requirments
  - Where are the weaknesses that cyber criminals exploit
    - Spoiler - it usually not the technology
  - List of the non-negotiable easy wins
- How do you prepare your firm
  - Resistant, Resilient and Responsible

Survey Findings

Survey findings

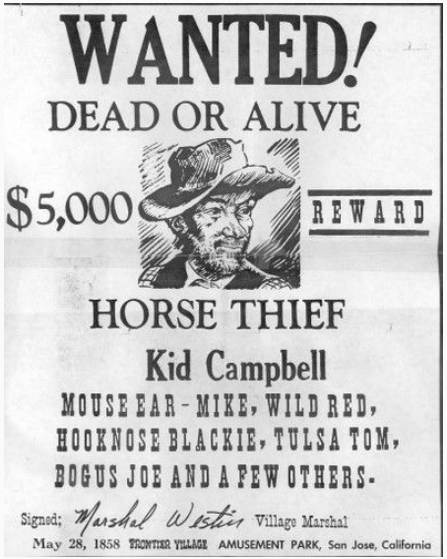
- The majority of respondent have been a victim of Cybercrime
- All respondents reported knowing someone

Common questions

- What is the relation between POPIA vs Cybersecurity
- Password management
- Encryption and VPN’s
- Is Cloud software a solution for security

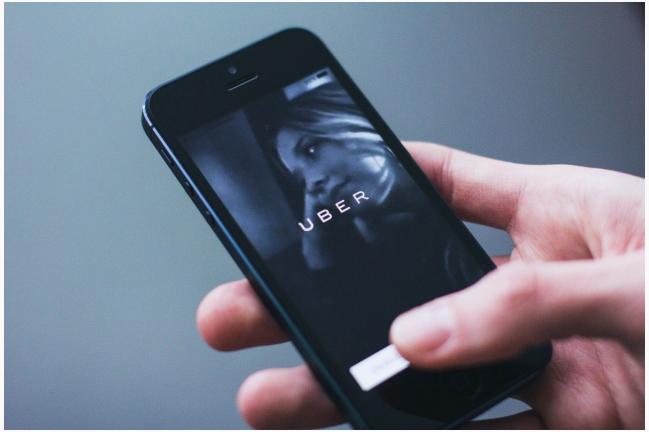
Motive

Cybercrime - more familiar than you think



Buying a stolen horse

Buying a stolen car



Buying an Uber with a forged credit card

Motive - Data is Money

Black Market Value

$15-$20 for a full personal identity

Full name, date of birth, address, phone number, mother's maiden name, ID number.

- What appears on a will or trust document
- Can be obtained from people's email account and social media account

Liability value (damages)

Loans and credit cards taken out in ones name

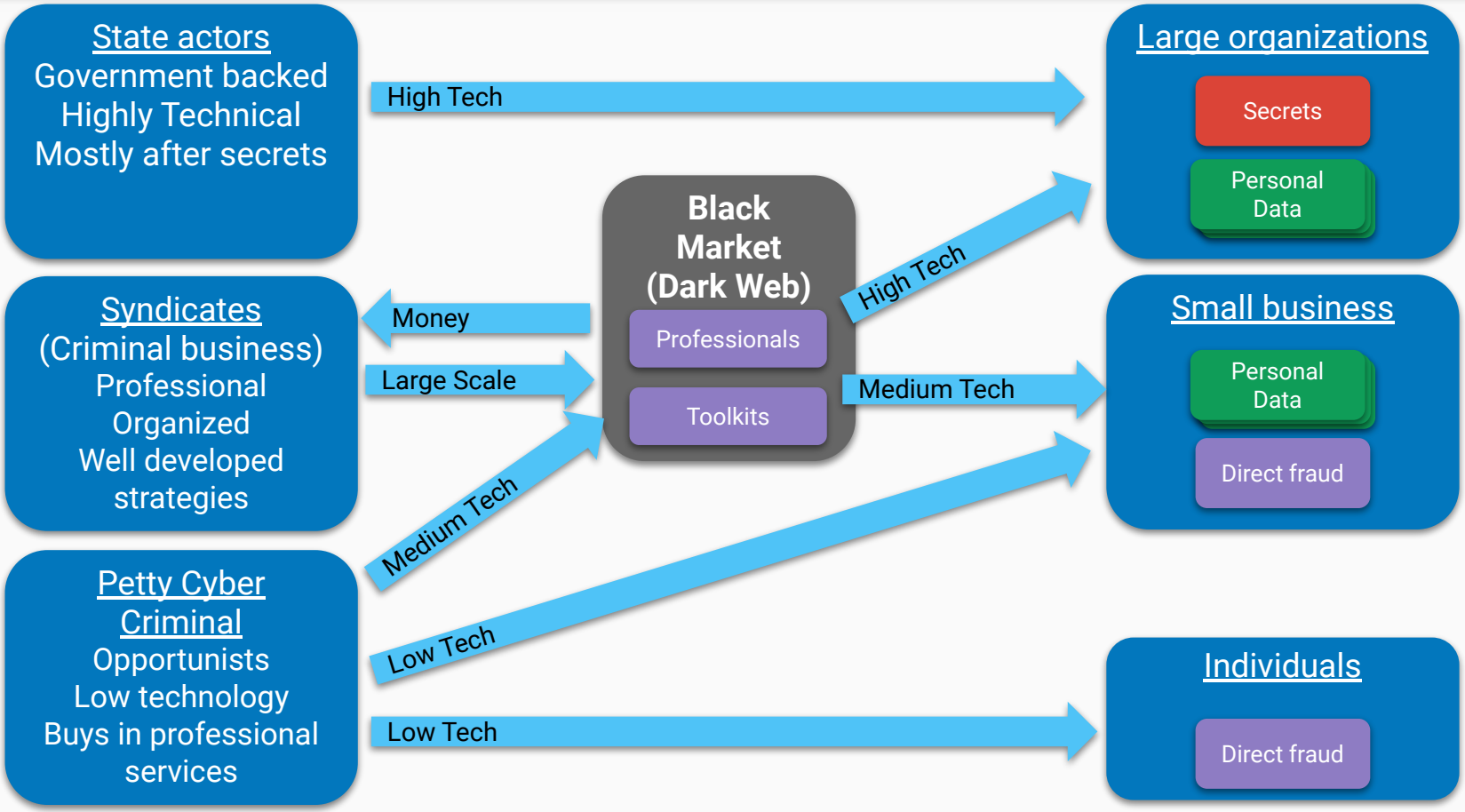
Bank accounts used for money laundering

Sources:

Black-market ecosystem Estimating the cost of "Pwnership"

2019 Black Market Report

Cyber Criminals and Targets



Examples of breaches

How was it done

What can we learn from each

IPMG

Cybersecurity is about technology right?

Most breaches occur via the following vectors:

- Human (Social engineering)
- Poor policy and enforcement
- Complacency

Breach Examples

1. Large Breaches (High tech)
    a. And how they affect small business security
    b. Simple mistakes that even larger organizations make
2. Medium tech breaches
    a. Emphasizing the importance of the human factor
3. Corporate complacency and poor policy
4. Case Study - Small Business Breaches
    a. Direct Fraud (spear phishing)
    b. Ransomware attack

Examples of Attacks - High Tech

1. Almost never directly targets small business
    a. Unless it is part of a large scale attack
2. Small businesses do not have the resources to defend against these attacks
    a. The best that can be done is to limit the damage and recover quickly.

- Example 1 - Marriott International (2016)
    b. Contained credit card and passport information for 500 million reservations
    c. Most likely a spear phishing attack, where the attacker knew what they wanted
    d. Went undetected for 4 years
    e. No fraud has been conducted using these materials (yet).
        i. State or corporate espionage
    f. Stolen by obtaining credentials from an internal IT administrator maintaining their reservations system

- Example 2 - Linked-in (2012, 2013, 2016)
    a. Repeated compromised due to failing to act on concerns from security researchers
    b. Attackers likely built tools to exploit flaws like these
    c. Attackers obtained personal details, along with usernames and passwords that insecurely stored by Linked-in.
    d. These are still for sale on the black market
    e. These usernames and passwords were then used to compromise accounts on hundreds of other services, where people re-use passwords
        i. Office 365 accounts
        ii. Corporate systems
        iii. Google accounts
        iv. etc

SA Largest data breach - Deeds Office

1. October 2017 - TimesLive
2. Security researcher Troy Hunt, obtained a copy of a “masterdeeds” backup file on the black market
3. It contained about 60 million records of South Africa property owners, 1990 - 2015
4. Property information, contact details, ID numbers, full names, employer information, marital status and estimated income.
5. The source was traced to a property group Jigsaw Holdings
6. Security researchers tested the security of their systems and found that they could gain access to a server containing the same information
7. Purchased from credit Bureau Dracore in 2014 to track down potential clients who might sell their houses.

What can we learn:

1. All the data to conduct identity theft today is available
2. The database was compiled for marketing purposes.
    a. Shows the importance of POPIA legislation preventing the sales of personal information
3. Do not blindly trust your IT professionals
    a. Regularly have their work reviewed and your systems tested

Latest prominent breach - Experian

1. August 2020 - Mybroadband.co.za
2. Experian is a credit Bureau used by many prominent South African banks
3. 24 million personal and 793,749 business details were exposed
4. This information came from various prominent banks, submitting credit checks of their clients.
5. The information was obtained by an individual fraudulently representing a client of Experian
    a. Experian provided the information in contravention of their security policies
6. The individual was apprehended and the information recovered.
7. It did however take months for them to detect the error

What can we learn:

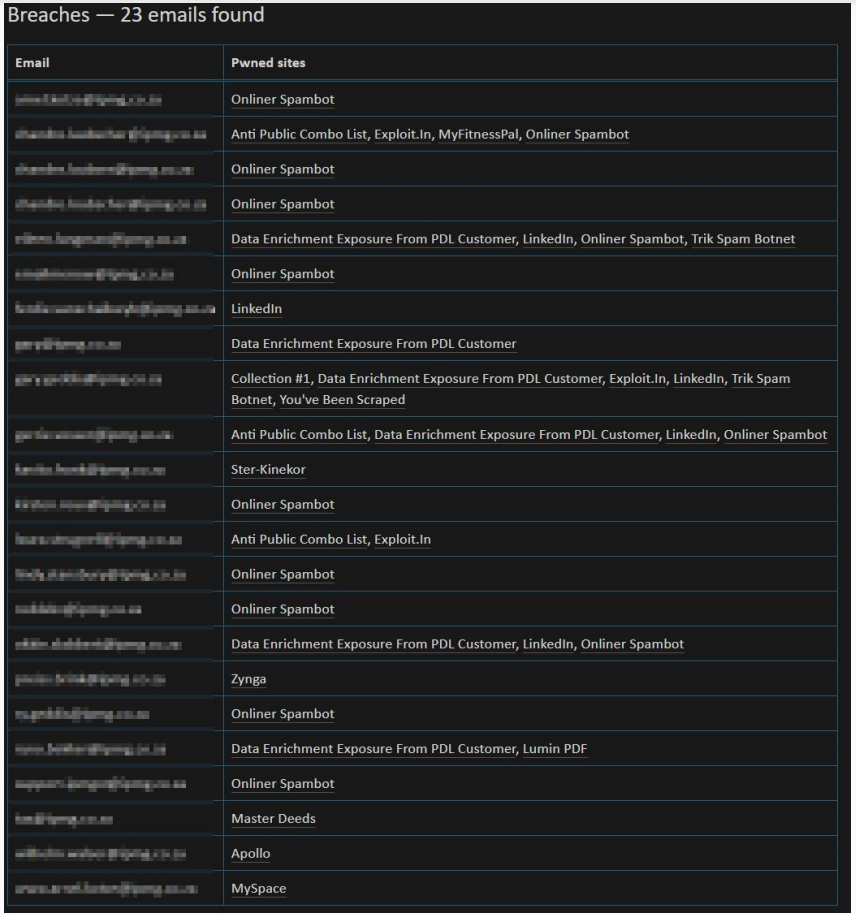
1. Experian lacked a secure method for authenticating a client request
    a. They got spear phished
2. Service providers due diligence is essential
    a. A simple “yes we have security” is insufficient
3. Ironically, Experian provides are Identity theft prevention and detection service
    a. Organization’s culture needs to support policy.

Has your information already been exposed

Online service to check

https://haveibeenpwned.com/

- Run by security researchers
- Funded by donations
- Also note you can setup notifications
    - Setup an alert for your business



Breaches — 23 emails found

Email	Pwned sites
[redacted]	Onliner Spambot
[redacted]	Anti Public Combo List, Exploit.In, MyFitnessPal, Onliner Spambot
[redacted]	Onliner Spambot
[redacted]	Onliner Spambot
[redacted]	Data Enrichment Exposure From PDL Customer, LinkedIn, Onliner Spambot, Trik Spam Botnet
[redacted]	Onliner Spambot
[redacted]	LinkedIn
[redacted]	Data Enrichment Exposure From PDL Customer
[redacted]	Collection #1, Data Enrichment Exposure From PDL Customer, Exploit.In, LinkedIn, Trik Spam Botnet, You've Been Scraped
[redacted]	Anti Public Combo List, Data Enrichment Exposure From PDL Customer, LinkedIn, Onliner Spambot
[redacted]	Ster-Kinekor
[redacted]	Onliner Spambot
[redacted]	Anti Public Combo List, Exploit.In
[redacted]	Onliner Spambot
[redacted]	Onliner Spambot
[redacted]	Data Enrichment Exposure From PDL Customer, LinkedIn, Onliner Spambot
[redacted]	Zynga
[redacted]	Onliner Spambot
[redacted]	Data Enrichment Exposure From PDL Customer, Lumin PDF
[redacted]	Onliner Spambot
[redacted]	Master Deeds
[redacted]	Apollo
[redacted]	MySpace

Real-world Case Studies
IPMG Data Breach investigations

IPMG

Small Business Attack 1

Spear Phishing

Real IPMG investigation no 1

IPMG

Why this example

1. Its a real world case investigated by IPMG
2. It is the most common example of Cybercrime we have encountered
3. There are many variations and can be adapted to many types of businesses
4. It is very low tech in terms of what the criminal needs to know.
5. Example of a “Petty Cyber Crime”

Preparation by Criminal

- Buy a list of compromised email addresses from the black market (500)
  - Filtered for South African companies
- Visit company websites to identify companies that are worth targeting
  - Sufficient size
  - Sufficient staff count
- Research company employees on social media networks
  - Who works for them
  - Who does business with them
- Set-up a bank account with fake identity (purchased online)
- Select final targets (25)
- Log into their email accounts and monitor their emails
  - Monitor for invoices
  - Setup email templates impersonating one or more creditors

Target - Spear phishing attack

Target: Sandy the Bookkeeper (also unofficial Financial Manager)

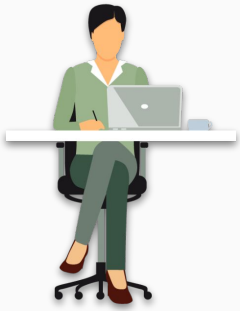
Works for John the business owner

She handles all the business finances as John is mostly focused on new sales and ideas

She loads supplier payments on the Internet Banking system

They buy their office supplies from 123 Stationery Suppliers about twice a year

Spear phishing attack



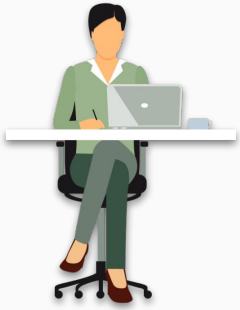
Placed their 6 month supply of stationary (R30k)

Email progresses to supplier normally

Compromised email is being monitored by criminal

Criminal prepares to intercept the invoice to conduct the scam

Spear phishing attack



Sandy receives the invoice with the modified bank details

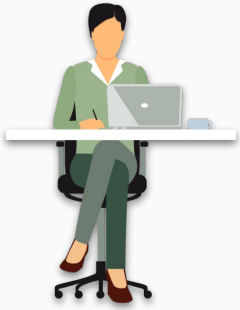
Supplier sends invoice for payment to Sandy

Criminal replaces email with modified invoice and a message about new banking details

Criminal removes email with invoice attachment

Criminal modifies the PDF attachment by putting a text block with new banking details

Spear phishing attack

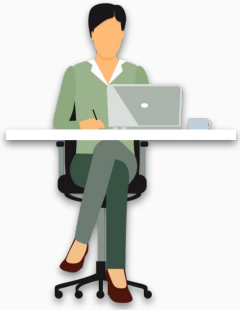


Sandy loads the payment on Internet Banking

John reviews and releases the payment to...

The criminal

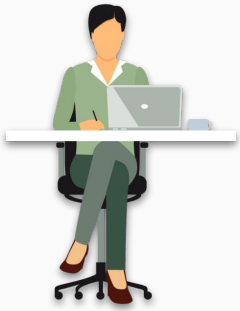
Spear phishing attack



Criminal uses cash-send functionality to send money to ATMs

It is collected in batches of R5000 from multiple ATMs

Spear phishing attack



3 Days later Sandy follows up with supplier

A few emails later they discover that the payment details were incorrect

Bank informs them that the money cannot be returned as it has been withdrawn as cash

How could it have been prevented

Customer

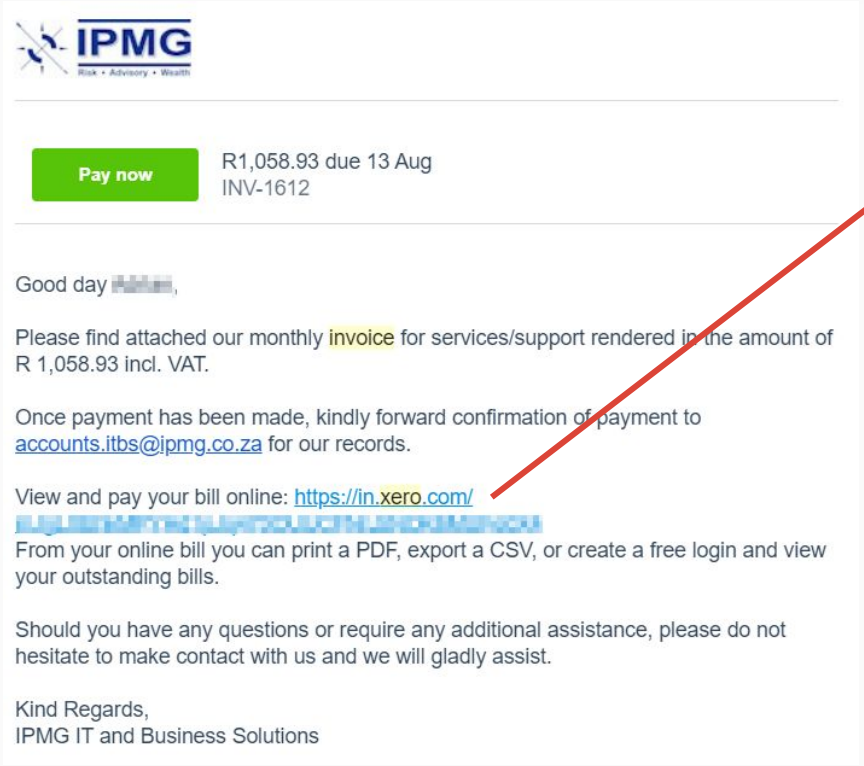
1. **They did not phone the supplier to confirm the change in banking details**
2. **Sandy used the same password on her email account as on her Linkedin account**
    a. Linkedin got hacked multiple times
3. They did not use an email service provider that has 2 factor authentication
    a. Like Google G-suite or Office 365
4. Did not deal with a suppliers that provides on-line payment options with:
    a. Better fraud protection from bank
    b. Much more secure than emailing sensitive information

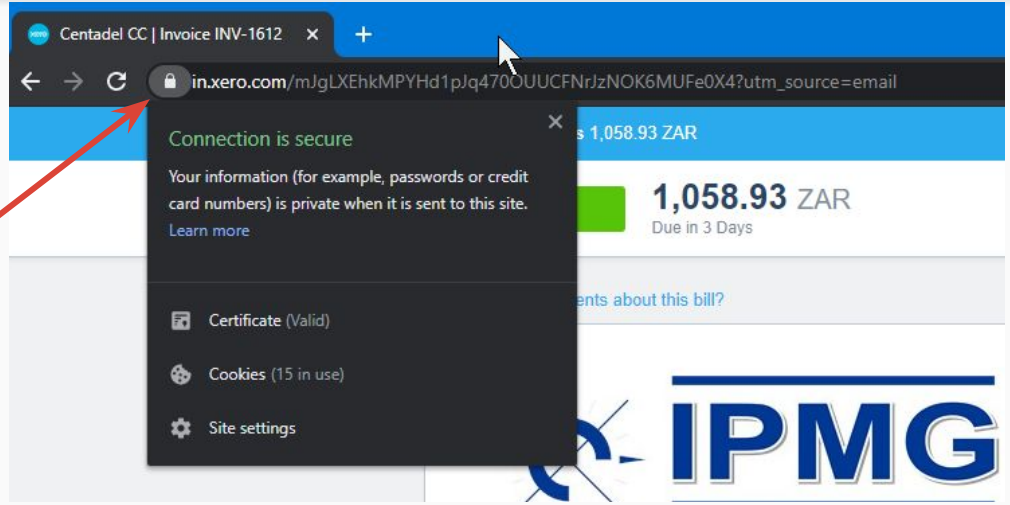
Supplier

1. They sent the invoice via email as a PDF attachment
    a. Both are easily modified

If <u>any one</u> of the above was implemented, the scam <u>would have been impossible</u>

Send Online invoices





1. Your web browser (unlike email) does an identity check to confirm the details are authentic
2. Emails sent by cloud accounting systems have extra security measures implemented
    a. Leading email service providers like Office 365 and Google G-suite will check for these measures before delivering the email

Password reuse

- MYTH - Changing a password regularly makes it more secure
- REALITY - It promotes password re-use across multiple services
  - Humans are not built for remembering dozens of passwords

Password Managers

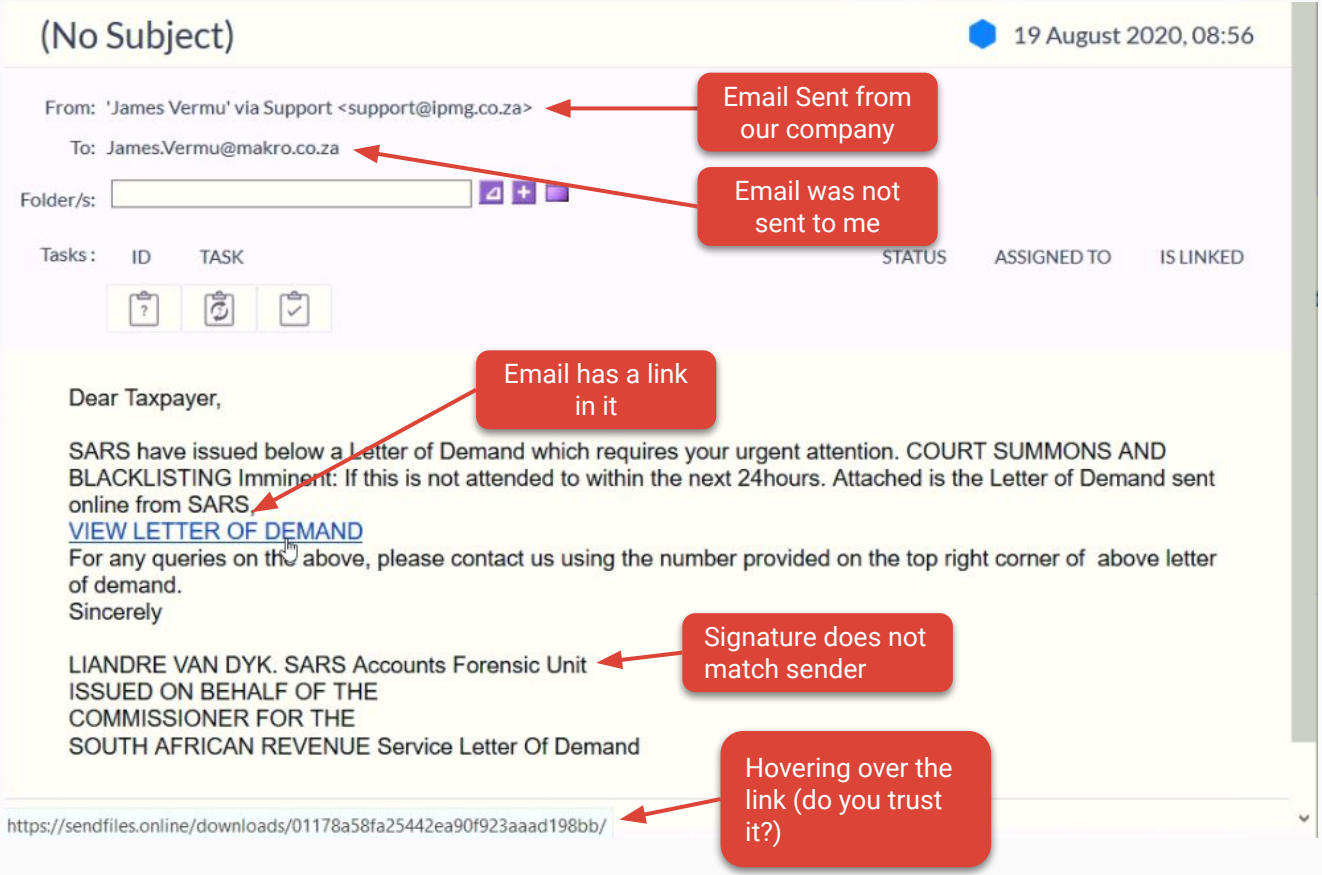
1. Solution to password re-use
    a. Generates passwords
    b. Makes them easier to use complex ones
2. Protects your passwords
    a. Encryption
    b. Two-factor-authentication
3. Allows for sharing of passwords between staff (Cloud offerings)
    a. Use shared passwords, without the ability to see the password
4. Checks your passwords against online services
    a. Lets you know if they have been compromised.
5. Event/Audit log
    a. Who used which password when

Examples

1. Bitwarden (www.bitwarden.com)
    a. Open source (transparent vetting)
    b. $2-$3 per user per month
2. Lastpass (www.lastpass.com)
    a. Largest commercial offering
    b. $4-6 per month
3. Keepass (www.keepass.info)
    a. Only your PC only
    b. Free and open source
    c. Store it on Google Drive, Dropbox, Onedrive to sync it across your devices
    d. Obvious upgrade from a spreadsheet, diary or on your cell phone

How to detect a scam

Scam email



This email has many many flaws, so why do they work?

1. People don't stop to think
2. Too busy
3. Too stressed

Everyone I have interview who got caught could spot their scam email

Reading links

Read from Right to Left

en.wikipedia.org

3rd-level domain	2nd-level domain (must be a unique combination with TLD)	Top-level domain (TLD, extension)
Something they picked for a function	Who owns the domain	Who is it registered with

What to watch out for

- Information sending services
  - https://send.files.com/kjahdkfjjkeituhgkc
  - https://mega.nz/file/1kjdfeoepf494#od
- Misleading Addresses
  - https://www.sa.rs/gov/za
  - https://sars.downloadfile.co
  - https://www.sarsonline.co.za

Small Business Attack 2

Ransomware attack

Real IPMG investigation no 2

IPMG

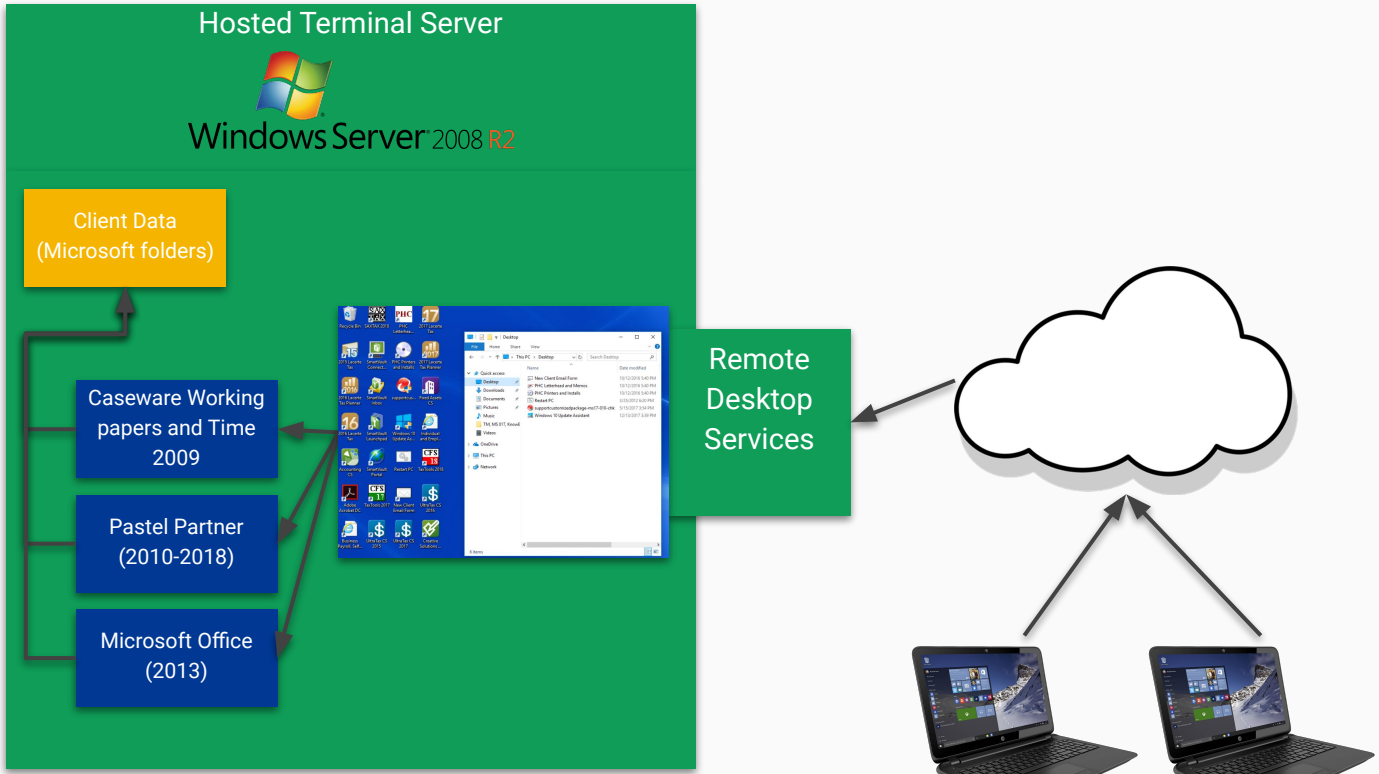
Why this example

1. Its a real world case investigated by IPMG
2. It demonstrate how business decisions affect Cyber Security
3. It demonstrates how professional criminal resources are used to breach business networks
4. We can also show how the gaps were fixed afterwards

The Target - Accounting firm

1. 2 Partners
2. 22 Staff
3. Working in 3 office locations
4. 5 years ago, they had 1 server in each office.
    a. Along with the difficulties in transferring files between offices
    b. And multiple software licences for each server
5. 3 years ago, they moved one of the servers to a data centre to consolidate and simplify their systems

Systems map - Before the attack (2018)



Security Measures in place

Security measures that were in place

1. Business Antivirus on all devices
2. Their emails were being scanned by an anti-malware service
3. Each user is required to have a sufficiently strong password
4. In-house IT professional (23 year old) maintaining it
    a. Worked between two companies with the same owners
    b. Generally well maintained, if under funded IT systems

Why they had the systems they had

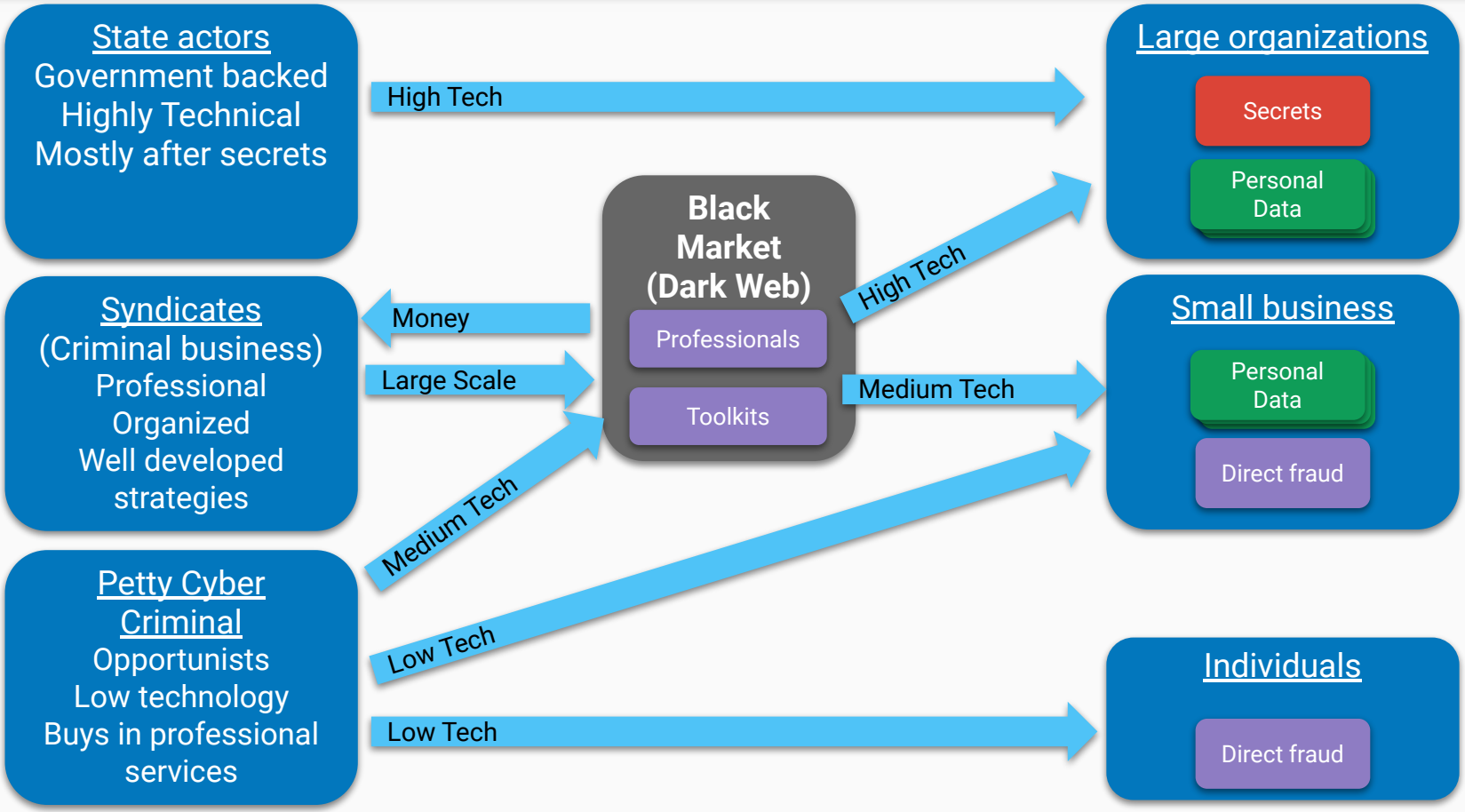
1. The business did not allocate much of the overall budget to IT systems and software
2. They had a very conservative approach to technology
    a. Hesitant to adopt more modern approaches like cloud software
3. They used a Remote desktop server for a variety of reasons
    a. Reduce IT capital costs
        i. Lower spec workstations
        ii. Only one server, not one in all 3 branches
    b. They did not want to transition from older Caseware working papers and Caseware Time to the latests versions
        i. They stated it was due to little to no functional benefits for a significant cost
    c. They still relied on Pastel Partner, which along with their other software was never designed to work across the Internet.
4. They were running an older version of Windows Server 2008 R2, since the newer versions were not compatible with their Caseware version

How the Criminal Prepared

Leveraging professional level criminal resource

IPMG

Cyber Criminals and Targets



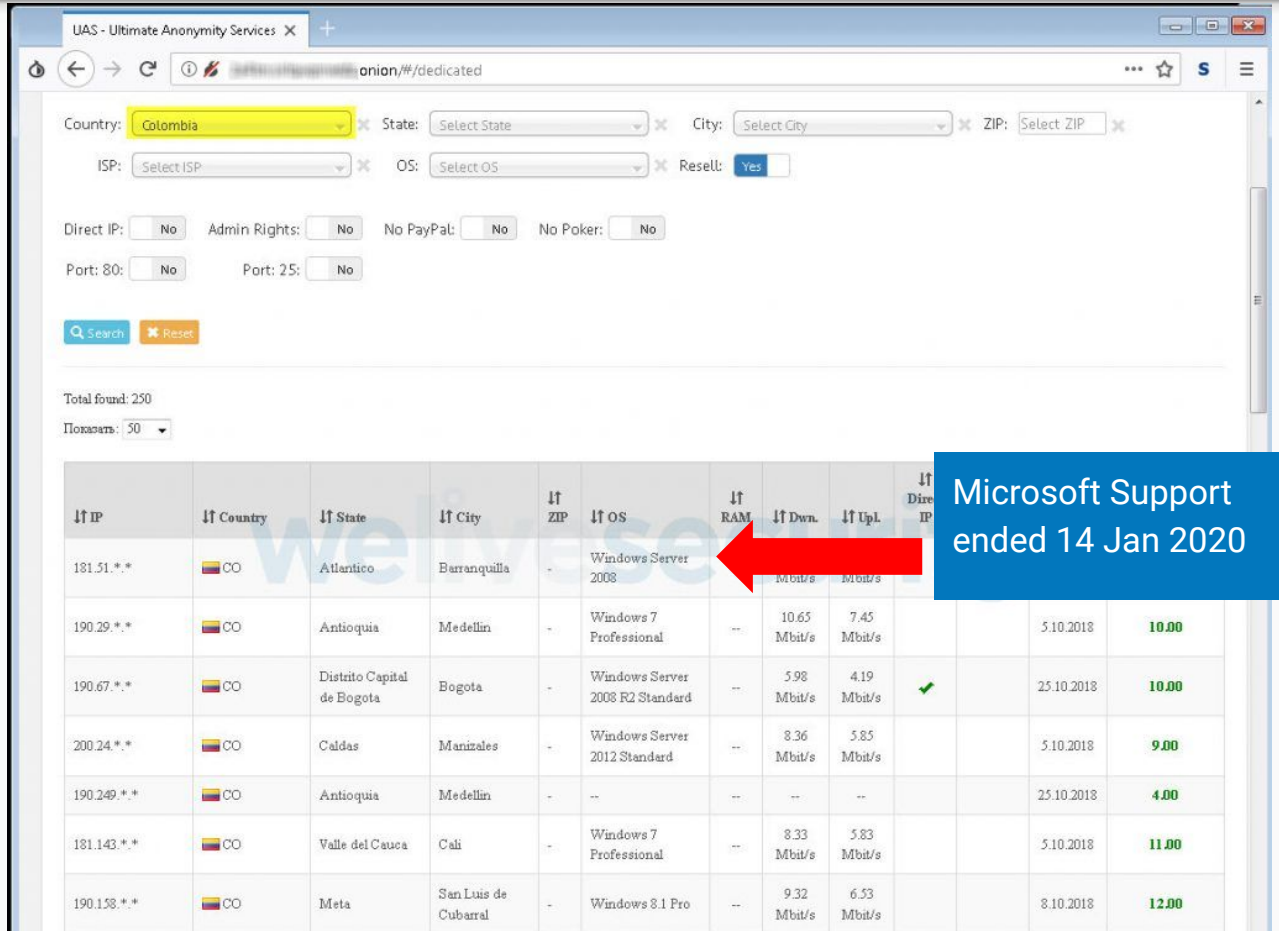
Shopping for Ransomware on black market

-= PACKAGES COMPARISON =-

	Package #3	Package #2	Package #1	Package #ELITE
Subscription	1 Month	6 Months	12 Months	12 Months
Darknet C&C Dashboard	Yes	Yes	Yes	Yes
Features: Delayed Start, Delayed Encryption, Mutex, Task Manager/Registry Editor Disabler, UAC Bypass, Desktop Wallpaper Changer	Yes	Yes	Yes	Yes
Offline Encryption	No	Yes	Yes	Yes
Support	No	Yes	Yes	Yes
Real-Time Client Manager	No	Yes	Yes	Yes
Dropper	No	Buy	Yes	Yes
Clone	No	Buy	Buy	Yes
FUD+Obfuscator	Buy	Buy	Buy	Yes
Unkillable Process	No	Buy	Buy	Yes
FUD Stub #	1	1	2	**12**
Price	120 USD	490 USD	900 USD	1900 USD

https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/

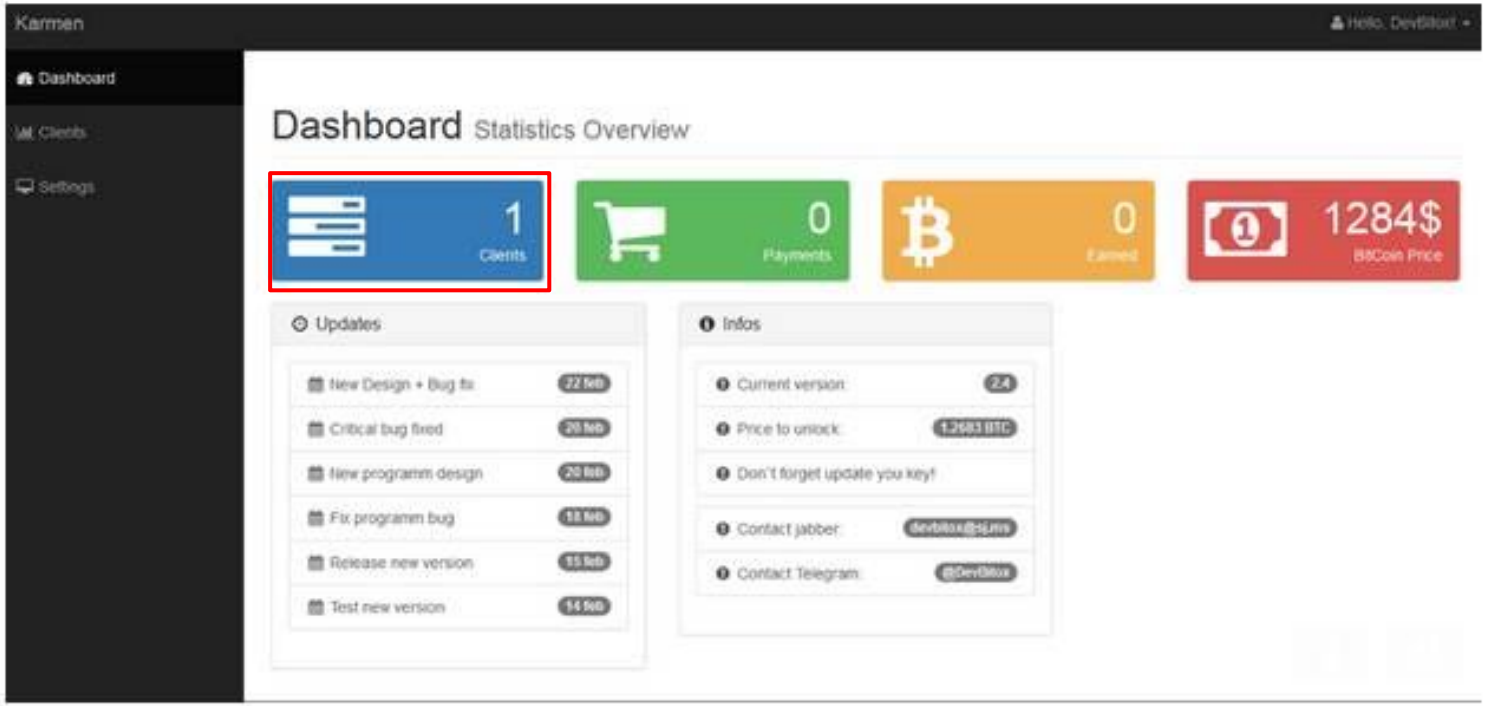
Selecting a target



1. Technical work of the reconnaissance was done by the syndicates
2. Server 2008 has an unpatched security weakness my ransomware can exploit

How to get into the server?

1. Try a known password list
2. Use the built-in tool that exploits any of known security gaps.



How the attack played out

IPMG

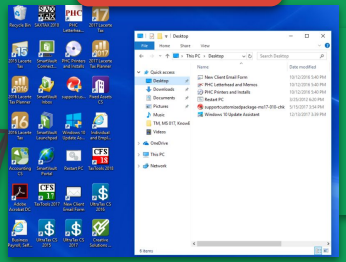
The Ransomware attack (2019)

Hosted Terminal Server

Windows Server 2008 R2

ENCRYPTED Client Data (Microsoft folders)

Ransomware



Caseware Working papers and Time 2009

Pastel Partner (2010-2018)

Microsoft Office (2013)

Remote Desktop Services

Likely gained access by exploiting vulnerability in old 2008 version of Windows Server

Ransomware Cloud service infrastructure

What happened next

1. They had excellent technical support to help you buy the bitcoin you needed to pay them
2. They would even decrypt some of your files
3. They were open to negotiation on a reduced price, since South Africa had a weak currency

What happened next

1. Their backups were also encrypted by the Ransomware
    a. The offsite backups were a week old
2. Thus they were forced to pay about $1800 in bitcoin
3. Followed by paying about R25k in labour fees to completely rebuild their entire infrastructure
    a. In case the malware was left behind after decryption
4. Lost about 6 business days in productivity
    a. R110k based on salaries
    b. Plus R240k in billable hours got deferred by 15 days
    c. Plus Late penalties for clients VAT
    d. Losses would have been 7-8 days more if they did not pay the ransom
    e. Extremely high stress levels for all in the business

Why were they breached?

Although the breach was technical in nature, **it was caused by business policies and decisions**

1. Running very old software
    a. Older than 5 years
2. Running software designed for traditional enterprise, not designed for the Internet
    a. Pastel, Caseware, etc
    b. Remote Desktop Services
3. Without sufficient mitigation strategies
    a. Protecting Remote desktop with a VPN
    b. Having a modern off-site backup system

Too conservative on their Information system decisions

How did they respond

SHORT TERM

1. Obtained peer review, by the insistence of their IT professional on the existing infrastructure
    a. “I am good at what I do, but I don’t know everything”
2. Improved their offsite backups
    a. Real-time Sync of data
3. Implemented a VPN solution

Cost Implication

1. About R9k pm in new expenses for these measures.
    a. Backup infrastructure
    b. VPN

LONG TERM

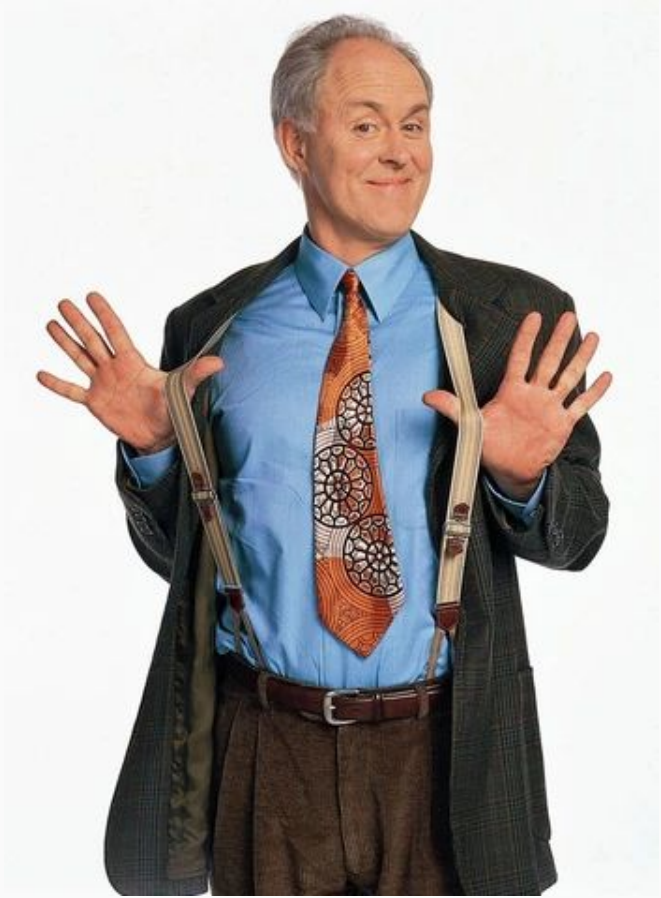
1. Committed to retiring their old software approach
2. Planned for modernization of their IT policies and decisions
    a. Outsourcing the security challenges to Cloud software providers
    b. Distributing their systems to prevent a breach from taking down the entire business

How would IPMG redesign their system?

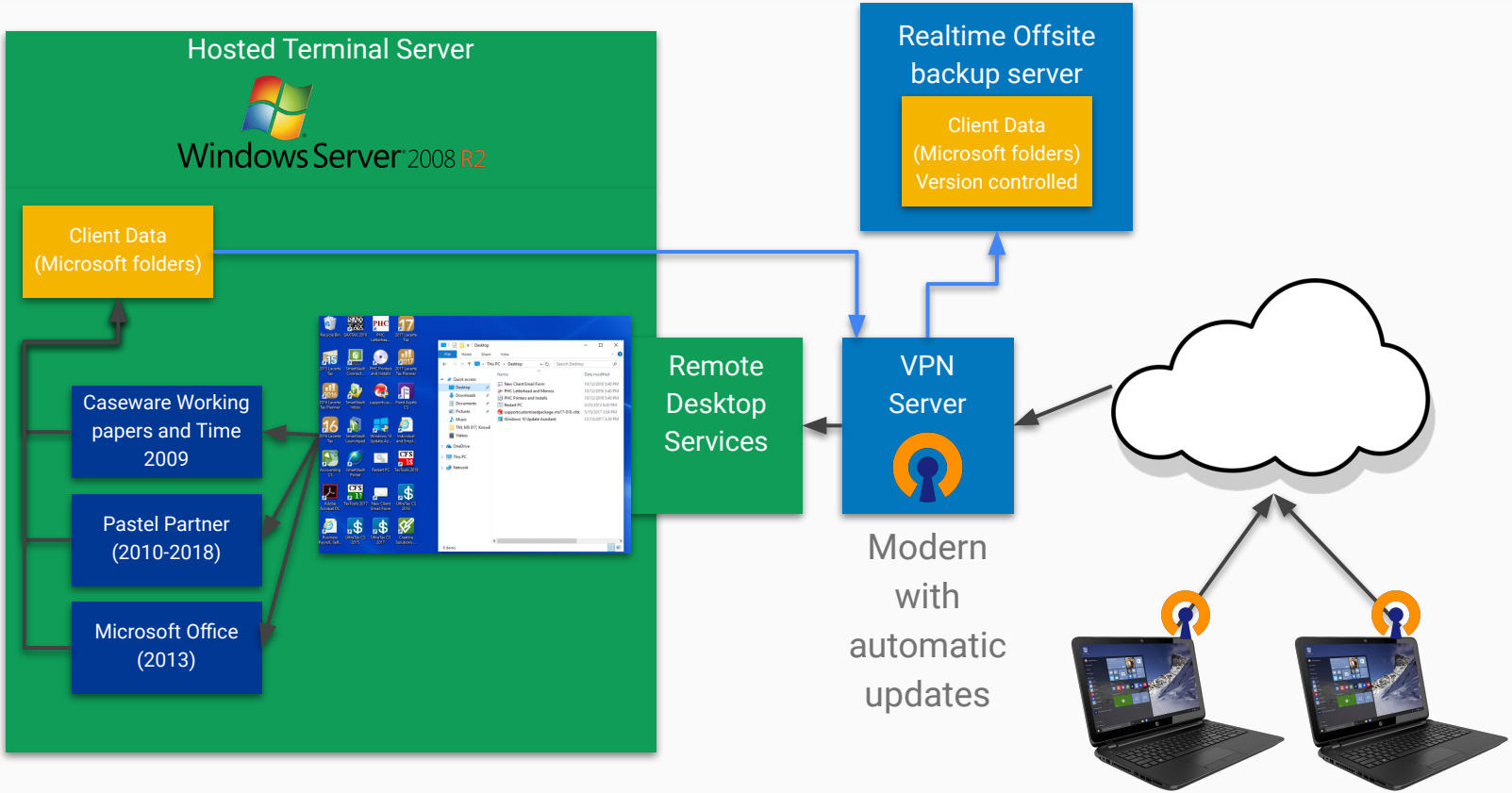
How do you secure known insecure systems

IPMG

How do you protect exposed systems



Systems map - Short term fixes



Limitations

1. Increase costs significantly
    a. R9k pm for the VPN and Offsite backups
2. Increased complexity
    a. Users have to connect VPN, which needs to be troubleshooted occasionally
3. No functional or productivity benefits

What have we learned from the two case studies

What have we learned?

Humans are the most exploited security weakness

1. Email is the most common method
2. Most of focused on obtaining passwords
    a. Use Password managers
3. Don't hesitate to manually verify the sender of an email
4. Migrate away from email for communication of sensitive information

Infrastructure Security is challenging and expensive

1. Against professional level criminal resources
2. Keeping older software secure is especially challenging
3. You need layers of security and cost
4. Sometimes the best you can do, is limit the damage and recover quickly
5. **Business decisions and policy directly affects security**

How to build a (mostly) secure cloud based business

Why Cloud?

1. Small business cannot compete with the professional level criminal resources
2. We need to rely on the security resources of larger organizations
    a. Microsoft, Google, Xero, Quickbooks etc.
    b. They have full time security professionals paid to combat the criminals
3. Given the increasing expenses to keep non-cloud infrastructures secure, the cost of cloud based software, is not a significant barrier to entry.
4. Cloud software, while technically more secure, have the same two weaknesses
    a. Human factors
    b. Poor Policy and Procedures
5. Those weaknesses are however, within your control to address
6. Aside from the security aspects, the automation, integration and productivity benefits are significant.

Questions to ask your Cloud service provider

1. Is 2 factor authentication available and standard for all accounts?
    a. Remember the lack of this, greatly increases the risk of password theft
2. Are all user actions recorded on an audit trail we can access?
3. Show me how I can limit access to information.
4. Are your developers and infrastructure engineers subjected to external peer review for security practices?
5. What assistance can we expect from you, in the event that we suffer a data breach with your product?

Non-negotiable & Easy wins

IPMG

Password Managers

1. Solution to password re-use
    a. Generates passwords
    b. Makes them easier to use complex ones
2. Protects your passwords
    a. Encryption
    b. Two-factor-authentication
3. Allows for sharing of passwords between staff (Cloud offerings)
    a. Use shared passwords, without the ability to see the password
4. Checks your passwords against on-line services
    a. Lets you know if they have been compromised.
5. Event/Audit log
    a. Who used which password when

Examples

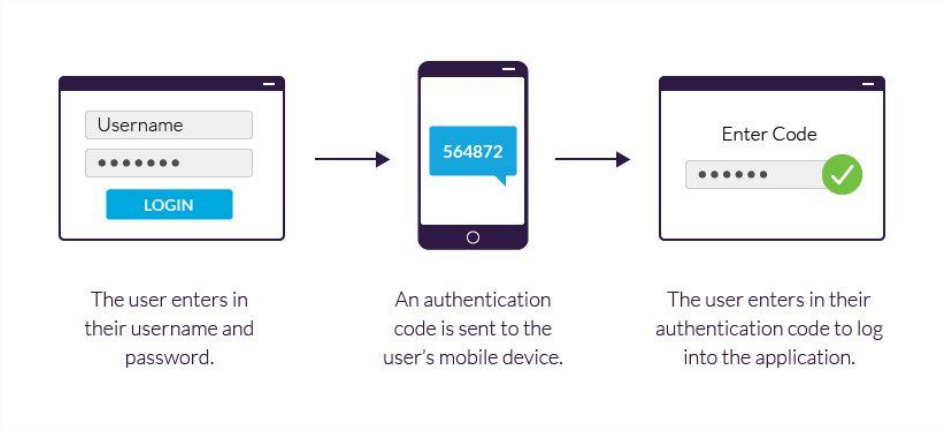
1. Bitwarden (www.bitwarden.com)
    a. Open source (transparent vetting)
    b. $2-$3 per user per month
2. Lastpass (www.lastpass.com)
    a. Largest commercial offering
    b. $4-6 per month
3. Keepass (www.keepass.info)
    a. Only your PC only
    b. Free and open source
    c. Store it on Google Drive, Dropbox, Onedrive to sync it across your devices
    d. Obvious upgrade from a spreadsheet

Staff awareness

1. Provide people with a list of things the business does not do via email
    a. Ask you to install software
    b. Ask for your password
2. People are going to make mistakes, don't expect them to be perfect.
    a. Encourage reporting of mistakes, even extend an amnesty for self reporting.
3. Discuss confidentiality and security on a regular basis.
4. Teach people how to understand a website address in an email
    a. Is the address from someone I trust?

2-Factor authentication

1. Best protection against password theft
   a. It requires the breach of 2 systems in order to gain access.
2. Only use On-line systems that provide 2 factor authentication
3. Pressure service providers who only offer it on higher end plans or don't have it at all
   a. Security should not be an optional feature
4. SMS is not not a secure 2nd factor, but better than nothing
   a. Sim Swaps are a growing problem
5. The best ones are app based
   a. From the app provider
   b. Or 3rd party like Google authenticator
6. Some apps allow you to force it on for all your users



Over-use of email

Why is email bad at security

1. It was never designed with security in mind
    a. Encryption is unavailable for most
2. Spam filters are not perfect
3. It creates copies of data you cannot control
4. Email, once sent is forever

What not to do with email:

1. Sending Passwords
2. Sensitive information
3. Attach unprotected sensitive information
4. Discussing confidential topics

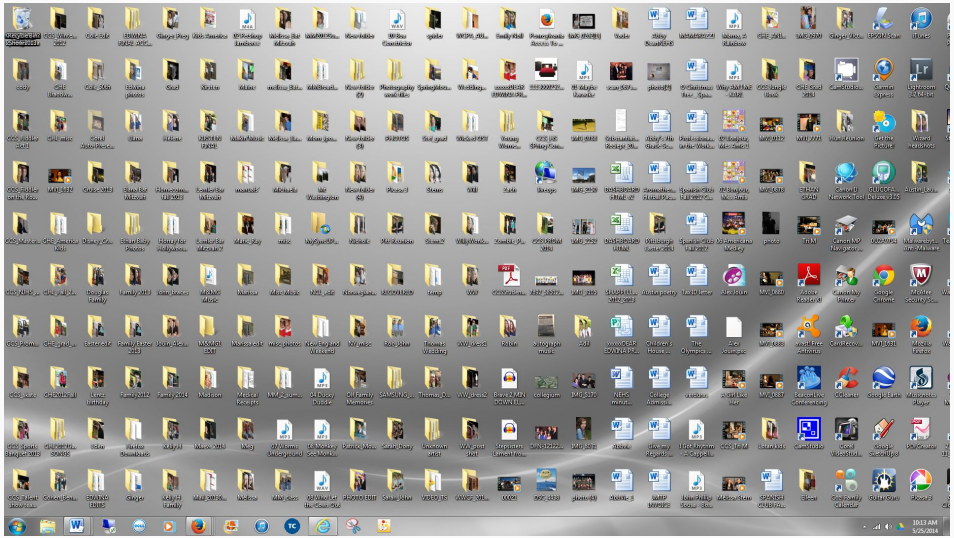
How do you improve email security

1. Providing links to documents instead of attachments
    a. Can be deactivated/expired
    b. Audit trail
2. Use Online documents
    a. Google docs and Microsoft onedrive/sharepoint
    b. Collaborate with the client there
3. Encourage clients to use secure Instant messaging
    a. They were designed with security in mind
4. Use a separate system for internal communication from what you use with clients

Adjusting Company Policy for Security

IPMG

Digital filing



We don’t accept this

Nor should we accept this

POPIA

POPIA was promulgated on 26 November 2013. POPIA is intended to promote the right to privacy in the Constitution, while at the same time protecting the flow of information and advancing the right of access to and protection of information.

What is the POPI Act timeline?

POPI commences on 1 July 2020. Giving you a 12 month grace period to get your organisation POPI compliant by the POPIA deadline of 1 July 2021. POPIA will be regulated by a new Information Regulator while within your organisation, your Information Officer is the key person to ensure compliance.

USE LEGISLATION AS A GUIDE FOR GOOD PRACTICE AND POLICY

Digital Filing Policy

1. Digital data should have authorized locations, workflows and access permissions associated with it. (Information Inventory)
2. Access to information should be restricted to the minimum number of people who should have access to it
    a. POPIA Requirement
    b. Limits the damage of data breaches
3. Have clear instructions for how sensitive information is exchanged with clients and 3rd parties.
4. These policies should be monitored for non-compliance
    a. Software is available to assist in this
5. Depending on the size and complexity of your organization
    a. Simple one page document
    b. Part of comprehensive employee handbook

Audit Trail is King

Treat client data like you would treat client money

- You would not purchase something without a receipt or invoice.
- Each action conducted on a piece of data should have a record of it in the system

Makes sure each person has a unique digital identity

- Do not share passwords between people
  - If you do need to share it, reset it after it was used.
- Do not share user accounts between people to save money on software.
  - Identity is the most important part of any audit trail.

Test your systems and policies

1. It is easy to become complacent
2. The first step is to self assess, to ensure that your systems controls and processes do not inadvertently subject your business to unnecessary risk
3. Consider having your systems, policies and controls independant, experienced professional
4. A good IT professional should welcome external peer review.
    a. It is not about pointing out their weaknesses, they should feel supported through that process. The goal is for everyone to learn.
5. Business should be part of the process.
    a. Improves awareness
    b. Promotes transparency in reporting
    c. Improves the quality of the outcome
    d. Be proactive and put your “best feet” forward

Breach Response Plan

IPMG

Do I need a plan?

As most of you have indicated, you have been breached, or know a client, or service provider who has been breached

Therefore, it would not be unreasonable to assume that a breach is possible, or even probable within some of your practices.

Being proactive means taking appropriate measures to protect your your client data and your practice, the best way you can.

It is greatly beneficial for all concerned to have a plan to guide then through what would be a very stressful incident.

Breach Response Plan

Contents of the Plan

1. Business Continuity and lockdowns
2. Communications
    a. Internal
    b. External
    c. POPIA and other regulatory requirements
3. Technical plan
    a. Assess and Arrest
    b. Recovering normal operations
    c. Audit and reconstruction
4. Cyber security insurance resources (optional)
    a. What will they do, what will we do
    b. How to activate the service

The size and complexity of your plan will depend your organization

Breach Response Team

1. Team leader
    a. Project Manager
    b. Decision maker
2. Technical manager
    a. Internal or external resource that conducts the technical aspect of the investigation
3. Communication manager
    a. Competent and confident (right personality)
    b. Handles all communication outside of the Response team
        i. Owners, Shareholder, Partners
        ii. Staff
        iii. Clients
    c. This person's role to to keep the external pressures off the response team so they can do their job

This team structure also applied to any other crisis the business might encounter

Communications

External

1. Have a pre-written response ready for clients, suppliers, regulators or media (sample)
    a. We have enacted our breach investigation plan
    b. We will comply with any regulatory, legal and law enforcement authorities
    c. We will contact affected parties (if any) directly
    d. If you have any specific concerns, please contact us directly so that we may address your concerns
2. Have a standard format for a breach incident report that complies with the requirements for POPIA disclosure

Internal

1. Ensure you have a separate system for communication with staff in an emergency
    a. Whatsapp Group(s) or similar system
2. Make sure they have a copy of any communication that they are allowed to state publicly, with confidence
    a. Refer any other queries to the communication leader
3. Ensure they know, what form of communication they can trust and who is leading the investigation.

Business Continuity and Lockdown

1. Have a lockdown plan in the event of a security breach
    a. Know which users are affected.
    b. Lockdown the data they have access to.
2. The Lockdown is managed by the response team.
    a. With full mandate to act on behalf of the company
3. If you are mostly using Cloud based services, your infrastructure is distributed and lockdowns will be very limited
    a. Unless your suspect password sharing or re-use may have been occurring
    b. Password resets of affected user accounts is usually sufficient.
4. If you have a “central server” with all client data and applications, a full lockdown will be required as all information is at risk with centralized systems.
    a. Re-open in phases as each user account can be verified to be secure.
    b. Be patient with the IT professionals doing the security checks. You cannot afford them to make a mistake.

Technical plans and reconstructions

Aside form the Business response plan, work with suitably experienced IT professionals to outline a technical response

1. It defines how they will respond
    a. Who would ideally have advanced mandate to ask for external assistance to ensure the best possible outcome
2. Provides them with a list of priorities to guide their actions
3. Any other arrangements necessary to speed up the response

In practice, many good IT service providers, lack the experience and confidence to handle an incident.

1. Do consider having an external service provider available to assist if required (peer review and support)
2. Or at minimum have the plan and your systems externally reviewed by professionals with suitable experience.

Recap

IPMG

Recap

1. Motives and mechanisms in cybercrime
2. Shown how large data breaches affect small organizations and individuals
    a. Identity theft and passwords
3. Two case studies of data breaches
    a. Exploiting the human factors
        i. Passwords and spotting a scam
    b. Criminal infrastructure
        i. How business decisions affect security
        ii. How to secure legacy systems
        iii. Difficulties in accommodating old software
4. Benefits of Cloud infrastructures
    a. Access to better security
    b. Questions to ask your cloud service provider

1. List of the non-negotiable and easy wins
    a. Password manager
    b. 2 factor authentication
    c. Sim swap mitigation
    d. Staff awareness
    e. The overuse of email
2. Data Filing Policies
    a. Better filing discipline dramatically improves security and reduces risk
    b. Information inventory
    c. Helps with POPIA
3. Importance of audit trails
4. Consider Independent 3rd party resources
    a. Opinions
    b. Additional capacity

Online self assessment

Below is a link to an IPMG form if you would like to request a on-line self assessment form

If your answers indicate that we may be of professional assistance to your firm, we may offer your a 60min complimentary consultation to discuss and advise you on your requirements.

We will also forward your feedback to SA Accounting Academy, which may inform future topics.

https://forms.gle/DnEWT9koNrATdUWA9

Thank you!
Any Questions?

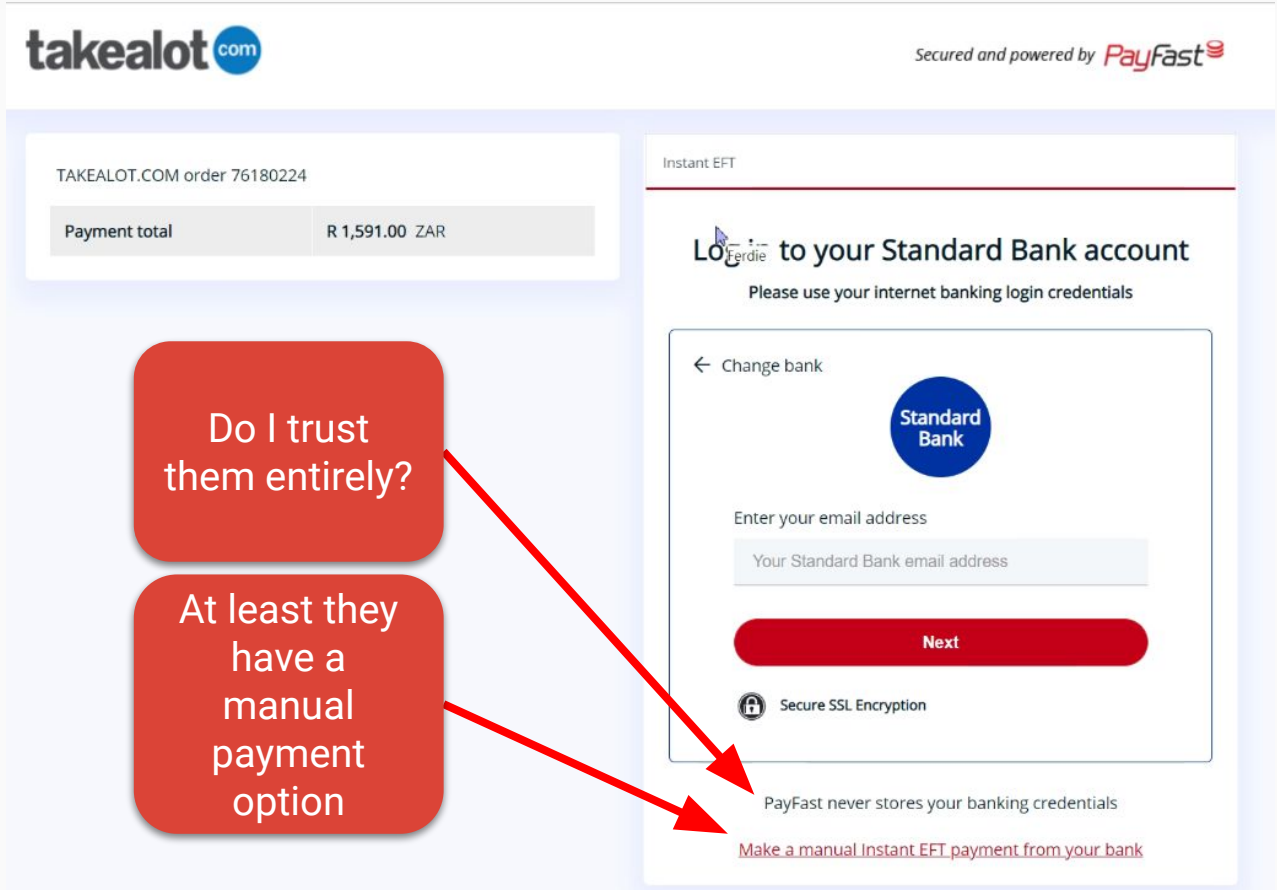
Please use the chat sidebar to the right of the video / presentation on the screen to ask your questions.

If you would like to e-mail a question please use:

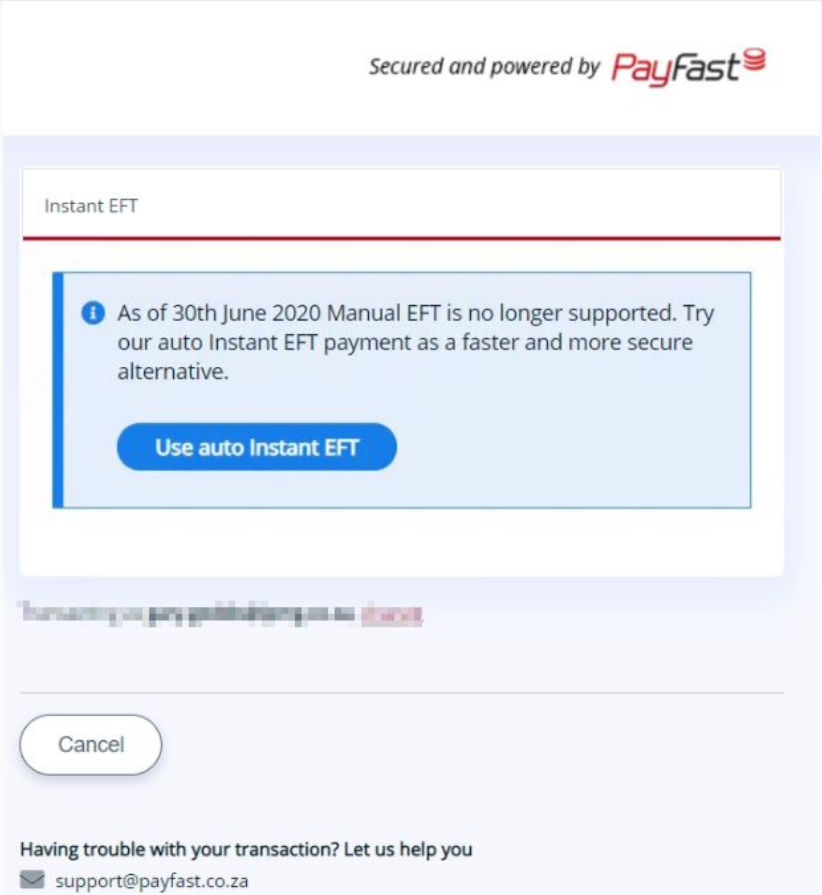
technicalquestions@accountingacademy.co.za

Supplementary slides

Business Complacency



Business Complacency



What can we learn:

1. Takealot selected two payment providers for non-credit card payment options
2. Both now require you to provide your internet banking details, so they can make payments on your behalf
3. Payfast had a manual payment option that did not require that I supply any 3rd party with internet banking details
4. They are stating that it is more secure to use their auto instant EFT option
    a. **More secure for who?**

Sim Swap mitigation

1. The cellular provider are not taking sufficient steps to protect your cellphone number from being stolen
    a. There is too much identity theft information available
    b. They rely on the same insecure SMS system
    c. They are not offering an alternative at this time
2. SMS's, like email, should be avoided as a method of authentication
3. Use the App based authentication from the service you are using
4. Or a 3rd party service, like Google authenticator
5. Pressure your service providers not to rely on SMS based authentication
6. **DO NOT IGNORE A SIM SWAP NOTIFICATION**
    a. Immediately phone your cellular provider

Encryption

1. Encryption is extremely useful for when data leaves your systems
    a. Backups
    b. Archiving
    c. Back-end breach
2. When data is being exchanged between back-end systems
    a. Doing online transactions (HTTPS)
    b. Sending data to a 3rd party
    c. Exchanging data between integrated systems
3. Encryption is of limited value if the system that is breached has access to the information via authorized channels
    a. This is why cybercriminals target users who have access (passwords)
4. Encryption of PC, Laptop and mobile devices are essential to mitigate physical theft (same applies to MFPs, server etc)
    a. Un-encrypted device theft will trigger the requirement for a POPIA breach notification
    b. Stolen laptops and devices are commonly mined for valuable data

File to Large for Google to Scan - Download Anyway ?