LSSA: AGM – 30 March 2019

Cybersecurity Considerations for Legal Practitioners

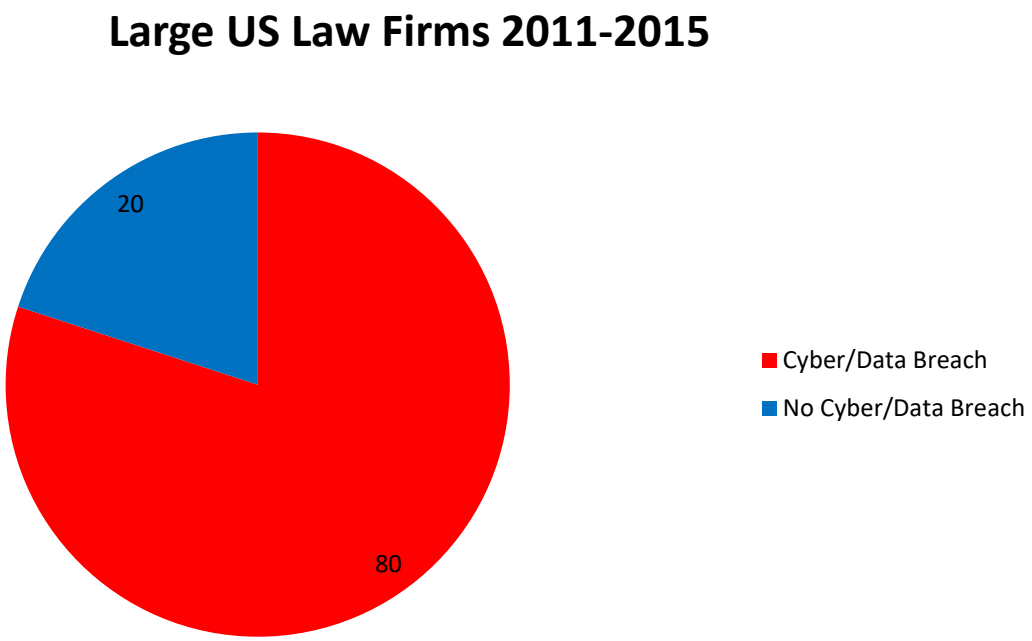
Preparing for when, not if, it happens!

PPM
Phukubje Pierce Masithela Attorneys

LAW SOCIETY
OF SOUTH AFRICA

Security: law firms are like gold!

Security: big/small practices are targets



- Cyber Attacks Upend Attorney-Client Privilege, Bloomberg

PPM
Phukubje Pierce Masithela Attorneys

Cybercrime – your practice is a target

PPM
Phukubje Pierce Masithela Attorneys

Why is cybersecurity important for your practice?

If not properly considered it can lead to -

Material financial loss through loss of productivity, of intellectual property, reputational damage, recovery costs, investigation time, regulatory and legal costs. This could lead to reduced competitive advantage, lower market share, impact on profits, adverse media coverage, bankruptcy, or even, where safety-critical systems may be concerned, loss of life.

PPM
Phukubje Pierce Masithela Attorneys

SALPC Rules Require Information Security Compliance

Rule 2.29 of the Rules for the Attorneys' Profession –

"*The Council and members shall ensure that all information, in whatever form, that is created, processed, communicated or retained (referred to in these rules collectively as "processed information") shall be processed subject to a degree of information security that is appropriate, having regard to the nature of the information and the purpose for which it is processed. In assessing the appropriateness of information security for purposes of this rule the Council and members must have regard to all applicable laws and rules, as well as relevant codes, guidelines and practices pertaining to the establishment and maintenance of information security.*"

PPM
Phukubje Pierce Masithela Attorneys

Implications of a breach for your practice?

- Downtime…think of all the firm's professionals unable to work;
- Loss of IP…your entire precedent base gone or confidential client IP stolen;
- Reputational…would your clients still have confidence in you;
- Operations…imagine all your accounting records being deleted;
- Legal Practice Council…what about disciplinary hearings before the LPC; and
- POPIA Information Regulator…breaches of personal info result in fines of R10 million or imprisonment.

PPM
Phukubje Pierce Masithela Attorneys

Laws, regulations and rules to consider?

- Rules for the Attorneys' Profession, 2016;
- Protection of Personal Information Act, 2013;
- The Electronic Communications and Transactions Act, 2002;
- The Regulation of Interception of Communications and Provision of Communication-Related Information Act 2002;
- South Africa's National Cybersecurity Policy Framework, 2015;
- King III – Code of Governance Principles in South Africa, Principles 12; and
- Information Security Guidelines for Law Firms, Law Society of South Africa.

PPM
Phukubje Pierce Masithela Attorneys

Cybersecurity: where do you start?

- As a small to medium law firm, with limited resources, what is expected of you? Section 19 of POPI gives some guidance:

(1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent-

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to-

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

PPM
Phukubje Pierce Masithela Attorneys

Cybersecurity: where do you start?

- Need not be a complex exercise in a smaller organisation. Five basic steps should suffice:
  - Make someone responsible for cybersecurity
  - Assess your risks;
  - Set up safeguards;
  - Select reliable and secure service providers; and
  - Continuous improvement.
- As you grow, expand on these steps to take into account more risks and need for stronger measures e.g. implement stands – ISO27001, Generally Accepted Privacy Principles (GAPP), etc

PPM
Phukubje Pierce Masithela Attorneys

Make someone responsible for cybersecurity

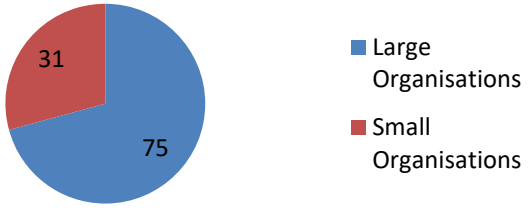
- Don’t bury your head in the sand…address the need;
- Define the person’s role;
- Ensure that they work closely with IT;
- If you don’t have IT at least outsource it;
- Develop basic cybersecurity policies, practices and procedures;
- Ensure that designated person and IT educate staff and make them aware of cybersecurity; and
- Person needs to ensure regular checks for compliance with policies.

PPM
Phukubje Pierce Masithela Attorneys

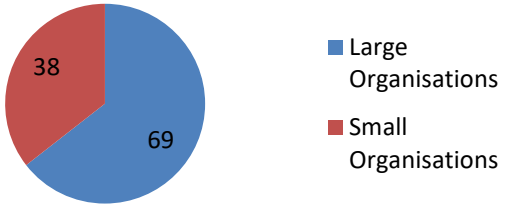
Assess your risk

- What sensitive/confidential information do you hold?
- How is it held: electronic or physical?
- Who has access to it?
- Take steps to evaluate reasonable internal and external threats: angry ex-employee; negligent candidate attorney; cybercriminals after client info.

Staff Related Breach



External Breach



PPM
Phukubje Pierce Masithela Attorneys

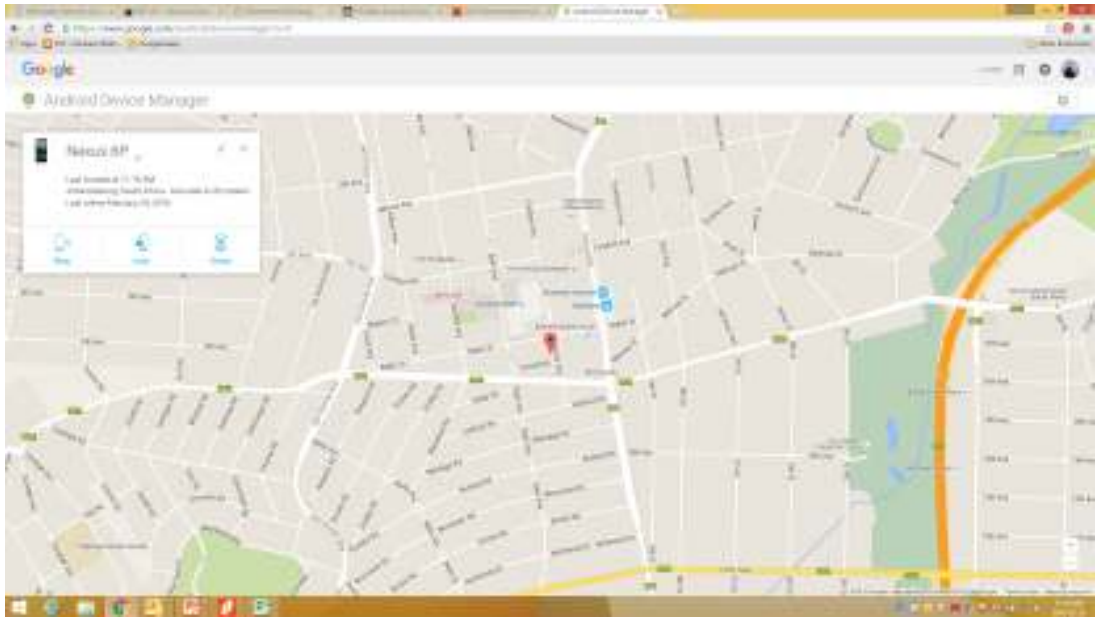
Set up safeguards

- Essence of a cybersecurity programme is "*taking appropriate, reasonable technical and organisational measures*".

PPM
Phukubje Pierce Masithela Attorneys

Safeguards: physical controls

- Locking filing cabinets/rooms;
- Keys – limit them to those who need them;
- Where are your computers, tablets & mobiles;



- Do you have alarms that work?

PPM
Phukubje Pierce Masithela Attorneys

Safeguards: administrative controls

- Background checks on staff;
- Training staff on firm's procedures;
- Special training for those who are mobile / work remotely;
- Be aware of how much you reveal about you / your firm.

PPM
Phukubje Pierce Masithela Attorneys

Safeguards: technical controls

- Passwords & password activated screen savers;
- Firewalls, anti-virus, spyware, patches – are they configured and up-to-date?
- Laptops, mobiles, back-ups encrypted…are there back-ups!

PPM
Phukubje Pierce Masithela Attorneys

Reliable & secure service providers

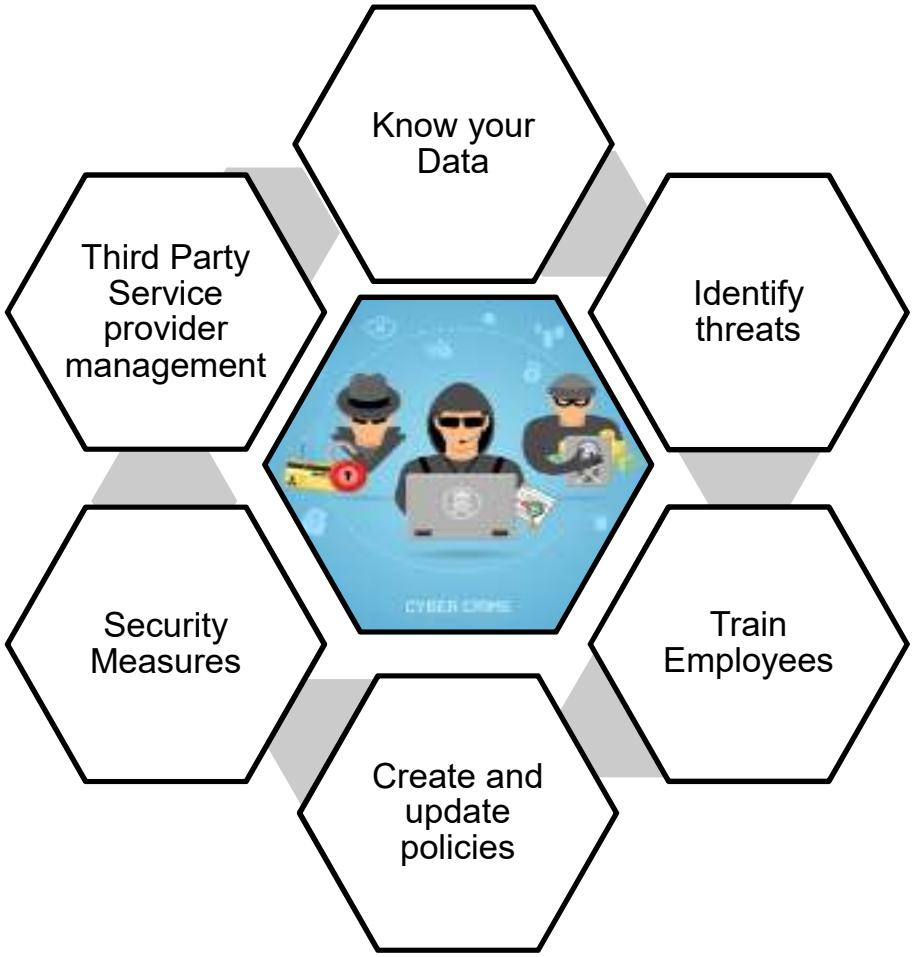
- Background checks;
- Service level agreement
  - Indemnities;
  - POPIA undertakings;
  - Minimum security requirements e.g. confidentiality. viruses, recovery of data ; and
  - Right to audit their services, hardware & premises.

PPM
Phukubje Pierce Masithela Attorneys

Example of an actual cyber-attack

PPM
Phukubje Pierce Masithela Attorneys

Preventing Cyber-Incidents



PPM
Phukubje Pierce Masithela Attorneys

Resources

- PPM YouTube channel
- PPM Website articles

"The POPI Act in 5 minutes: practical tips on organisational...
89 views • 2 months ago

I tweet what I like: employee disclaimers on social media -...
167 views • 2 months ago

Restraints of trade in the South African context
79 views • 2 months ago

PPM Attorneys Family MTB Day - 2015
75 views • 3 months ago

PPM Family MTB Day Competition Draw
41 views • 5 months ago

Social Media and Freedom of Expression
130 views • 10 months ago

IT Controls in the South African Public Sector - Tips on...
63 views • 11 months ago

How Hackers 'Pick you up' - Phishing Scams and What to...
98 views • 11 months ago

Social Media in the Workplace: Important Tips in the South...
65 views • 11 months ago

The DTI Film Incentive.
53 views • 1 year ago

PPM
Phukubje Pierce Masithela Attorneys

Any questions?

Follow us on:




PPM
Phukubje Pierce Masithela Attorneys