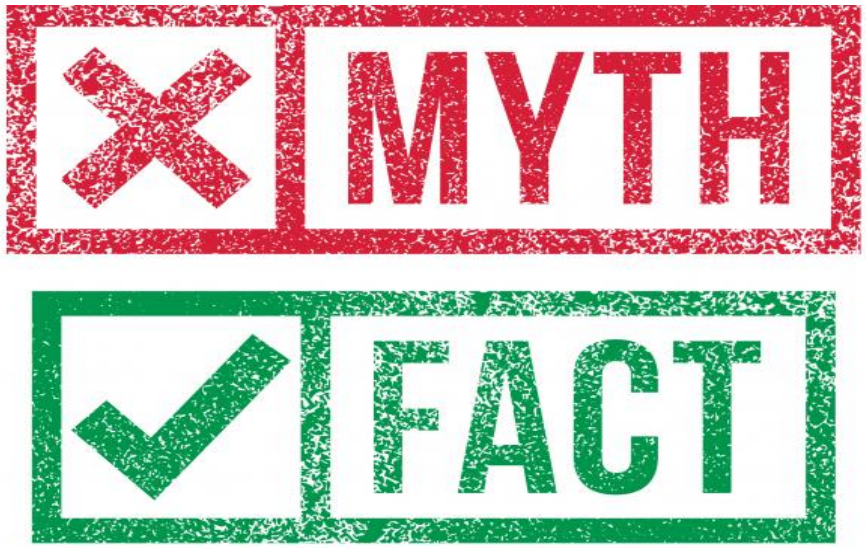
Cyber Security Myths and Facts

Michiel van der Wardt

IAP 75 24 May 2022

Cyber Security



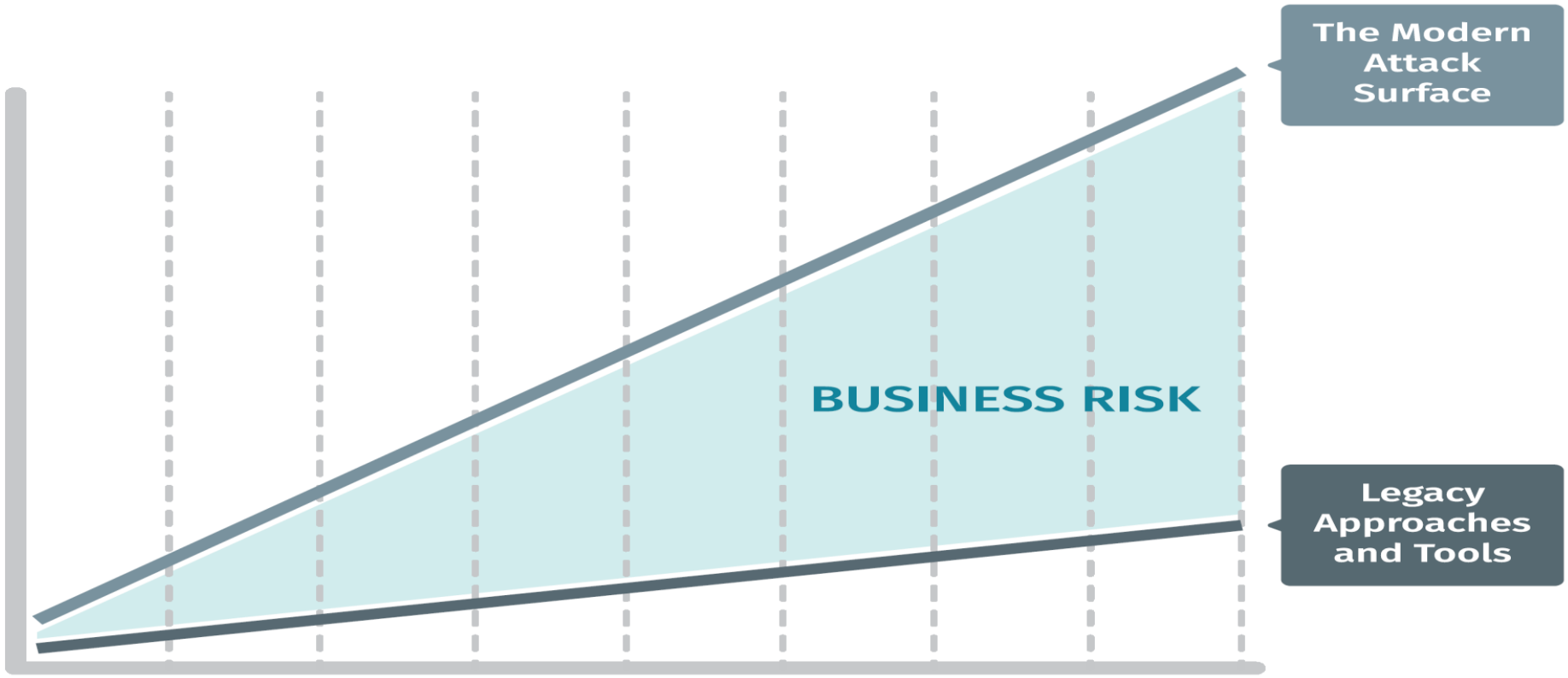
Michiel van der Wardt

IAP 75 24 May 2022

Myth 1
“We never experienced Cyber Attack, so cybersecurity should be OK”

Fact: Not IF, but WHEN

Cyber exposure gap



Protection does not keep up with attackers' developments

Myth 2

“Our Passwords are strong enough”

Username: admin
password: admin

Username: KoLpVXriw
password: l*$j">?ui$5

How Safe Is Your Password?

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

statista

2 Factor Authentication (2FA)

- Password + code sent to device
- Seen as a best way to protect online accounts
- If password is somehow hacked, still not able to access account, because of external code

BUT

2 Factor Authentication (2FA)

- ✕ Man in the Middle tools (free tool, used more and more)
- ✕ Placed in between your computer and website's server
- ✕ Allowing hacker to steal all data sent by server

Should we rely on IT services companies?

- IT services are non-core and can be outsourced
- Hiring own highly specialised IT staff can be tricky
- Always get service of 1st line technicians with required skills and experience
- Work with proven protocols

Hence:

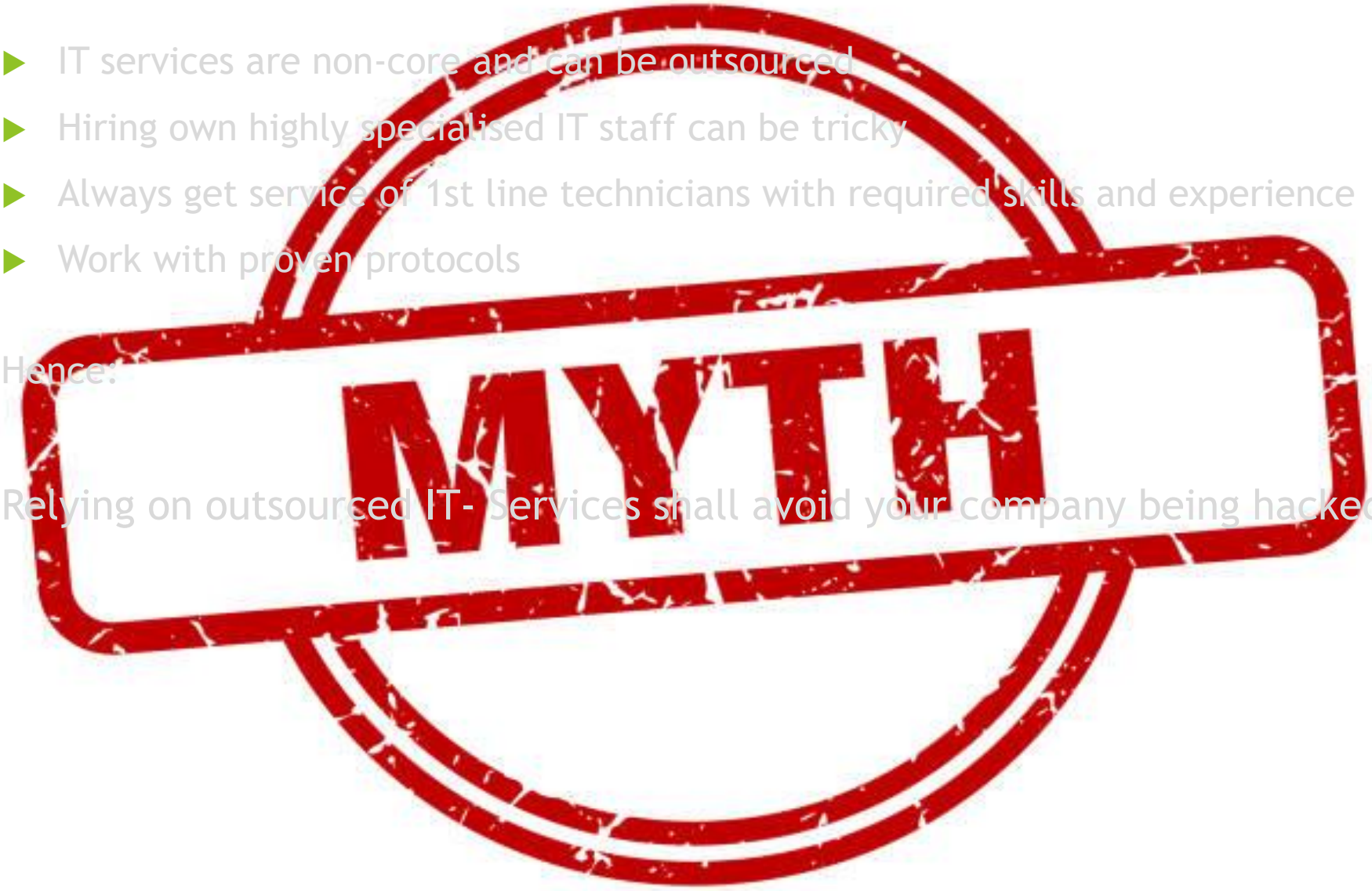
Relying on outsourced IT- Services shall avoid your company being hacked

Should we rely on IT services companies?

- IT services are non-core and can be outsourced
- Hiring own highly specialised IT staff can be tricky
- Always get service of 1st line technicians with required skills and experience
- Work with proven protocols

Hence:

Relying on outsourced IT- Services shall avoid your company being hacked



Fact: IT Services Companies can be hacked

- Dec 23 2019 IT service provider Synoptek got infected with ransomware
- Hackers Compromised Synoptek and infected 100 dentist practices that are client of Synoptek
- Couple of days before the attack, Synoptek posted on Twitter:

This text has been removed shortly after the attack

Is Paying ransom the best way to get back to business after hack?

- Loss amount for paying ransom only concerns the paid Ransom
- Upon payment of ransom amount, all locked files will be unlocked

Hence:

Relying on outsourced IT- Services shall avoid your company being hacked

Paying ransom is the best way to get back to business after hack.

?

Paying ransom is the best way to get back to business after hack.

- ✕ Loss includes paid ransom, downtime and lost work (and GDPR fines if applicable)
- ✕ Up to 20% of companies that pay ransom never geta access to all of their data
- ✕ Data may have been copied for later use (GDPR-impact)
  and
  Backup files may have been damaged

Should companies insure against ransom?

Insurance payment will reduce loss and protect.

BUT

- ✕ If ransom is paid, good reason to hack again
- ✕ Hackers are inclined to look for insured targets
- ✕ Also insurance companies can be hacked
- ✕ Insurance does not cover fines for leaked data (GDPR-breaches)

Should companies insure against ransom?

Myth 6
“Cyber threats only come from external actors”

Myth 6
“Cyber threats only come from external actors”

Fact: also internal human factors

- Employee negligence
- Employee ignorance
- Disturbed labour relation

Myth 7

“You know it immediately if your system is compromised”

Myth 7

“You know it immediately if your system is compromised”

Fact: it can take months or years to realise that your system has been compromised.

Myth 8
“We have achieved complete cybersecurity”

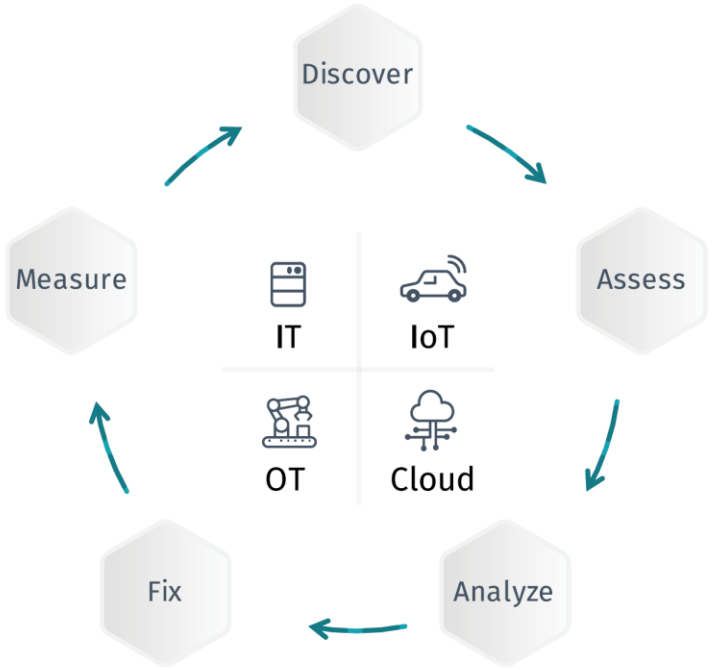
Fact:

Cybersecurity is a process

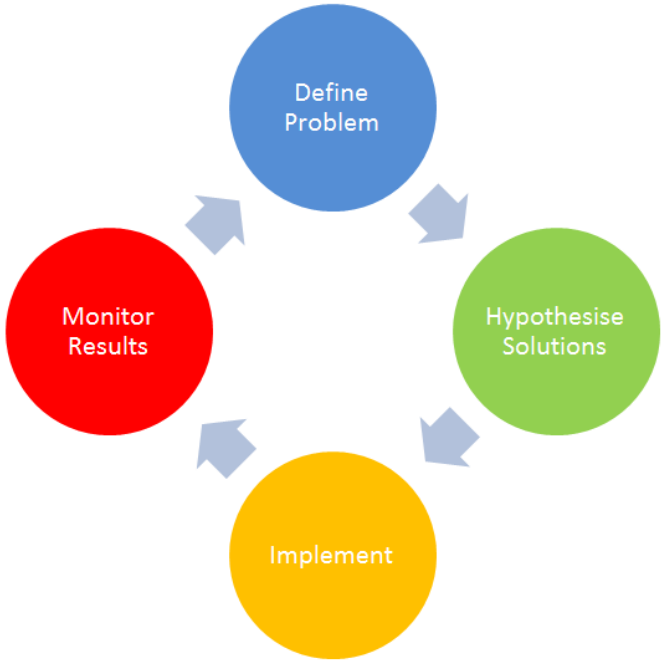
Not a state.

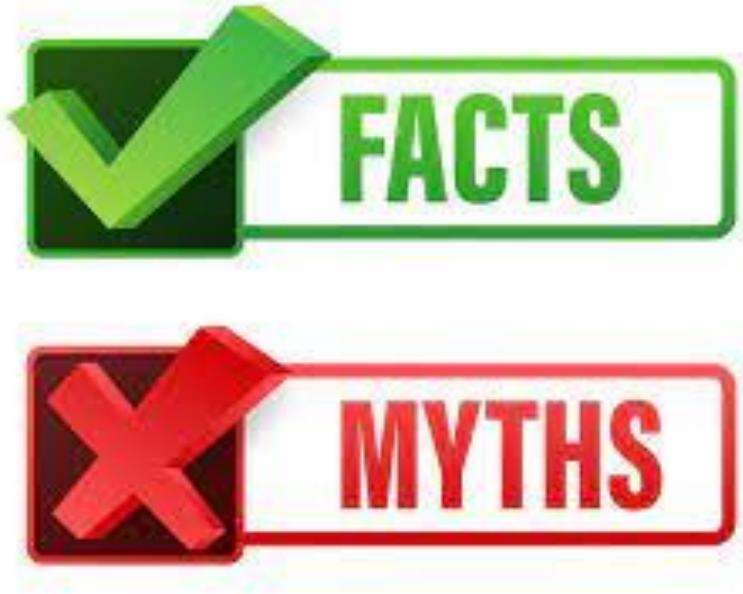
Cyber Risk Life Cycle resembles known territory

Cyber risk life cycle



Actuarial Control Cycle





Questions?

Michiel van der Wardt
Actuarial Risk Management Services
E: schadeactuaris@hotmail.com
T: +31 652 69 1625