Cyber risks and the life science industry

Presented by CFC Underwriting

June 2019

cfc

cfc | Cyber

Pioneers in cyber insurance

With nearly 20 years' experience in cyber insurance, CFC was one of the first companies to offer cyber insurance and has one of the largest cyber underwriting teams in the world. Our award-winning cyber insurance products are trusted by over **40,000 businesses** in more than **60 countries**.

CFC's dedicated in-house cyber incident response team is backed by a panel of expert global response partners and operates the world's first cyber incident response app.

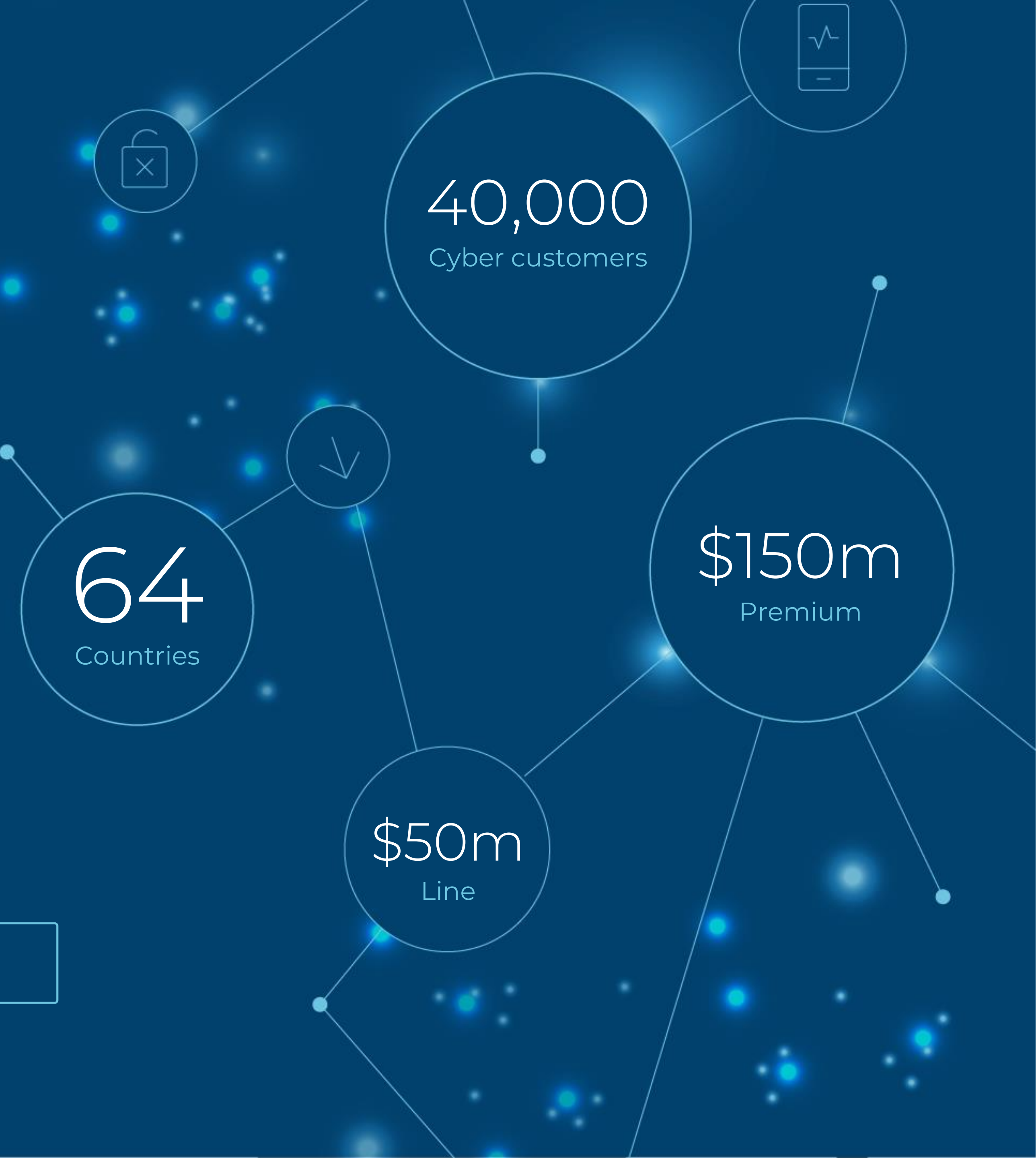
Our cyber products

Private enterprise

Large corporate

Healthcare

*Cyber cover is also offered as standard on most CFC policies



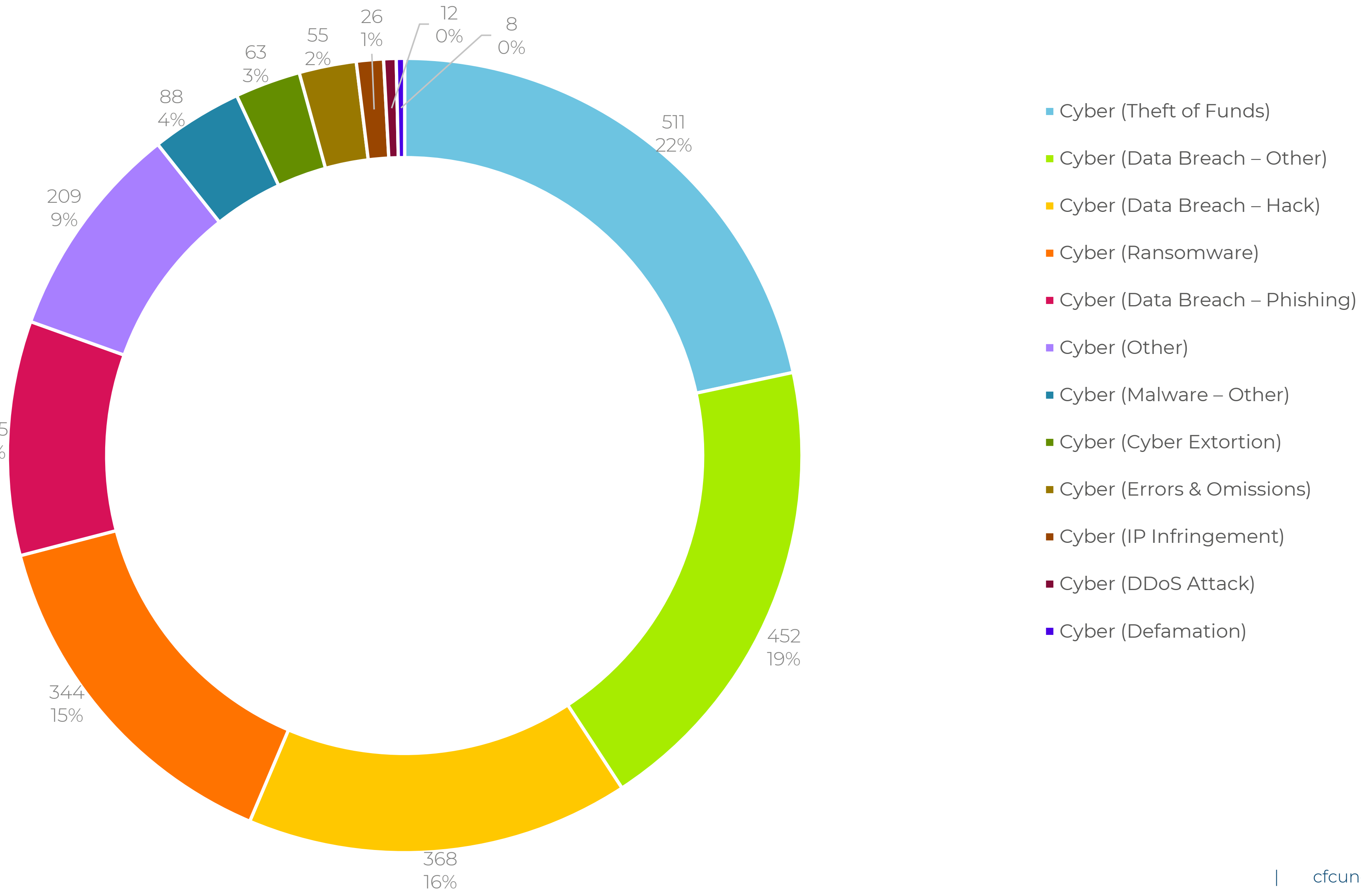
40,000
Cyber customers

64
Countries

$150m
Premium

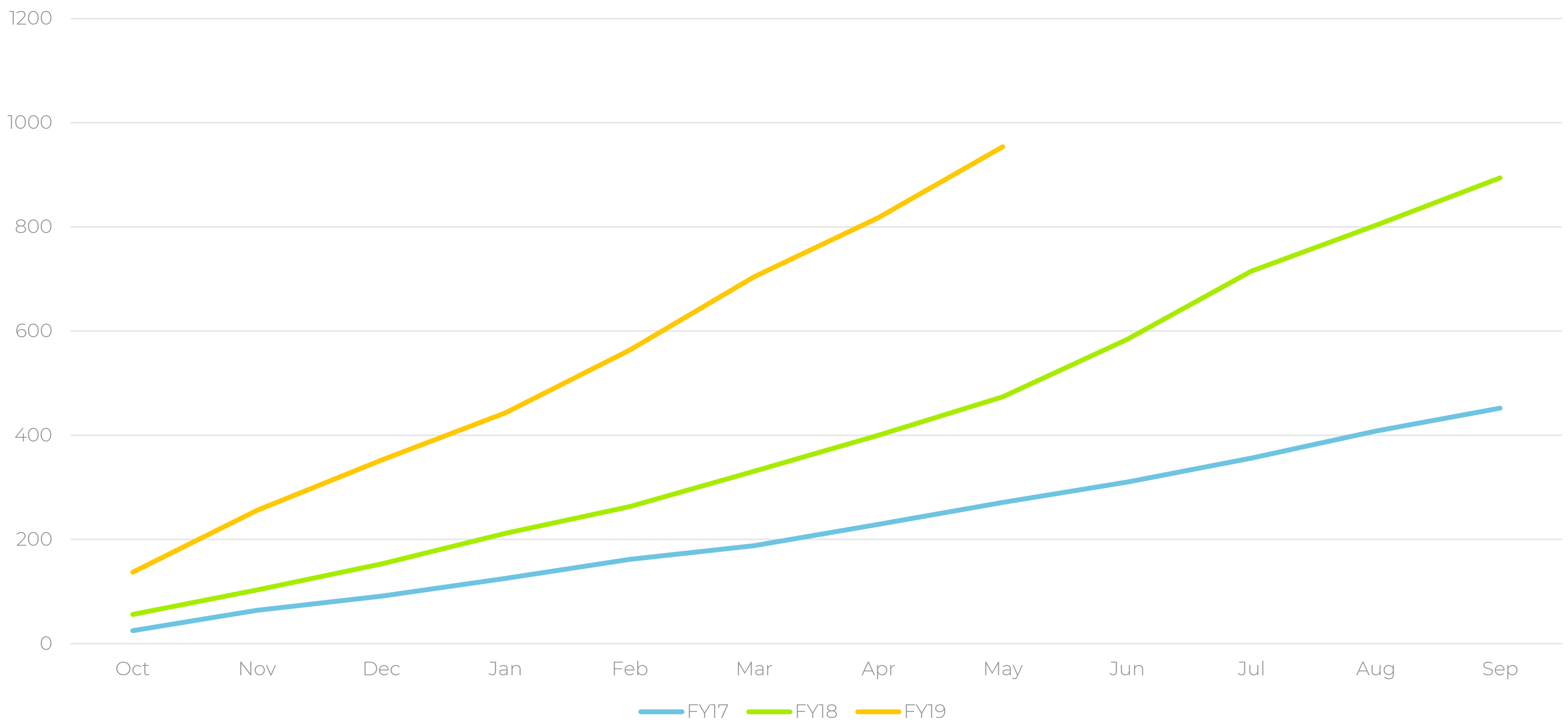
$50m
Line

Cyber Claims by Frequency 2016 -2018



Cyber claims volume is up significantly year on year

Cyber claims volume comparison



Digitisation

1 The importance of data

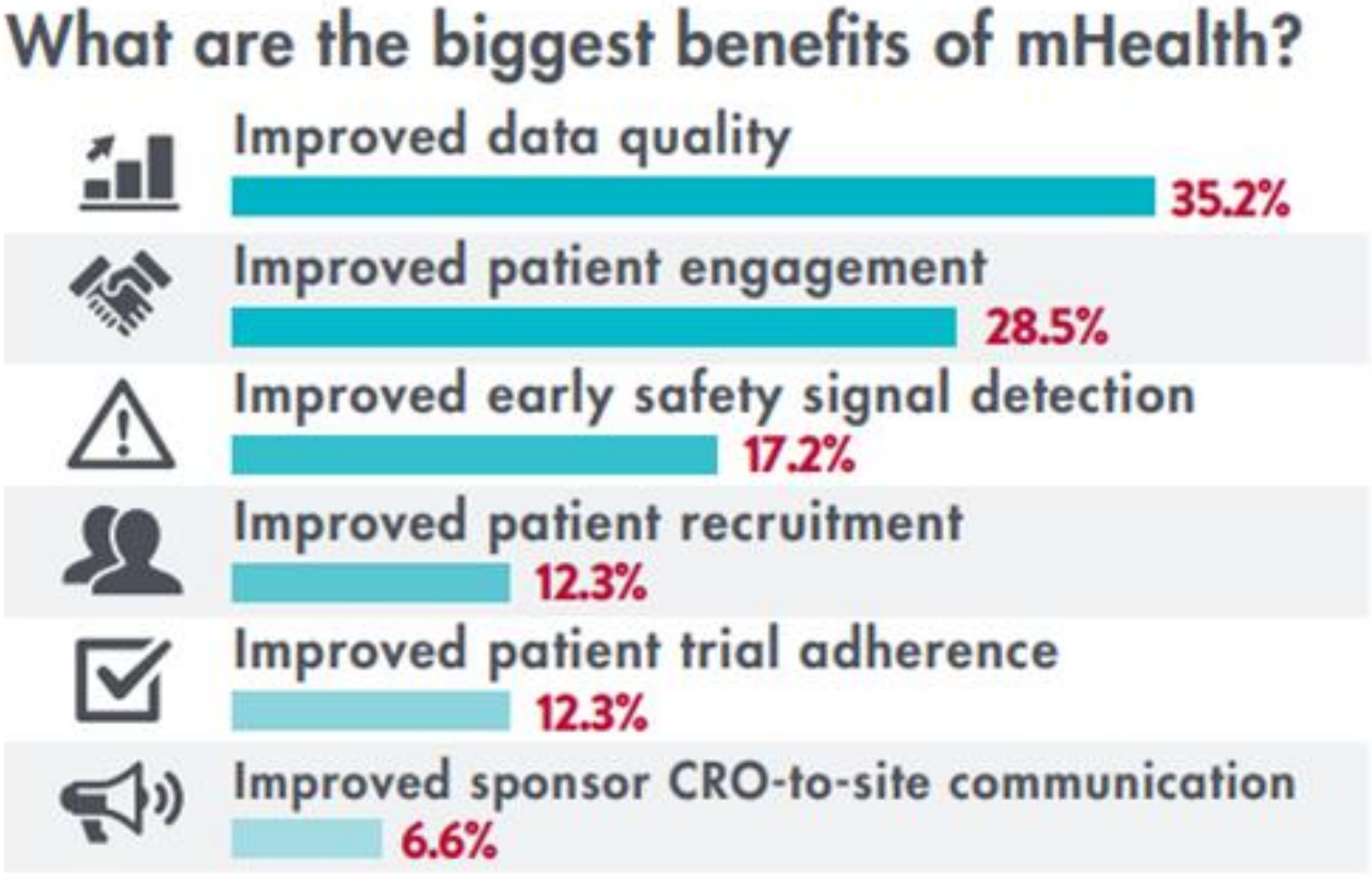
2 Reducing costs

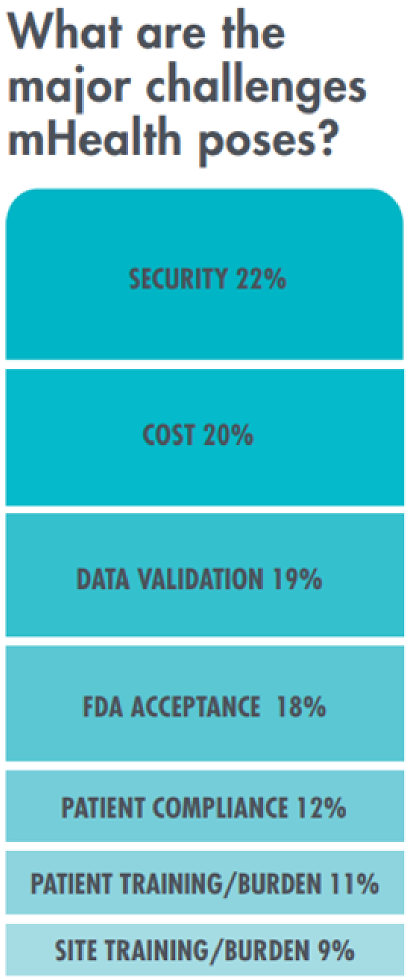
3 Reducing errors

4 Faster route to market

cfc

Data sharing – benefits and challenges





Source: SCORR Marketing and Applied Clinical Traisl : https://www.scorrmarketing.com/wp-content/uploads/SCORR_ACT_Mobile-Health-in-Clinical-Trials-Survey-Report.pdf)

What do life science companies really value?

1 Investment funds and/or fee income from the sale of products or provision of services

2 Physical and intangible assets

3 Reputation

4 Continuity

1 Biotech – development company

2 Clinical research organisation

3 Manufacturer

What can go wrong?

1. Electronic theft of funds
2. Loss or theft of intangible assets
3. Temporary or permanent loss of data
4. Loss of patient data
5. System downtime

The biotech

1. Classic nil revenue business
2. Evidence of clinical safety and efficacy
3. Virtual business model – reliant on vendors
4. Managing investor expectation – delivering on milestones
5. Protecting intellectual property

cfc

The biotech: claims review

1 Social engineering – CEO fraud

2 Extortion – loss of data

3 Theft of data

cfc

The service provider: CRO

1 Big data, proprietary software and data capturing

2 Outsourcing of expertise to vendors

3 Reliability and robustness of data - damage to reputation

4 Loss of patient healthcare data

CRO : claims review (system damage and BI)

1. Data re-entry and data re-creation
2. Loss of income and ICOW
3. Consequential reputational harm

cfc

The manufacturer: claims review

1. Protection of manufacturing know how
2. May hold third party intellectual property
3. Theft of funds
4. System downtime impacting the manufacturing run
5. Bodily injury and vulnerability of devices

Vulnerability of devices

1. Any product connected to another electronic device or network
2. Frequency in hacking attacks to healthcare organisations leading to in increase in data being compromised
3. FDA and EMA require cyber security to be part of risk management – Pen testing, confirming the presence of vulnerability, patching etc.
4. Does post market surveillance include cybersecurity review?

cfc

What can you be telling clients?

Loss mitigation

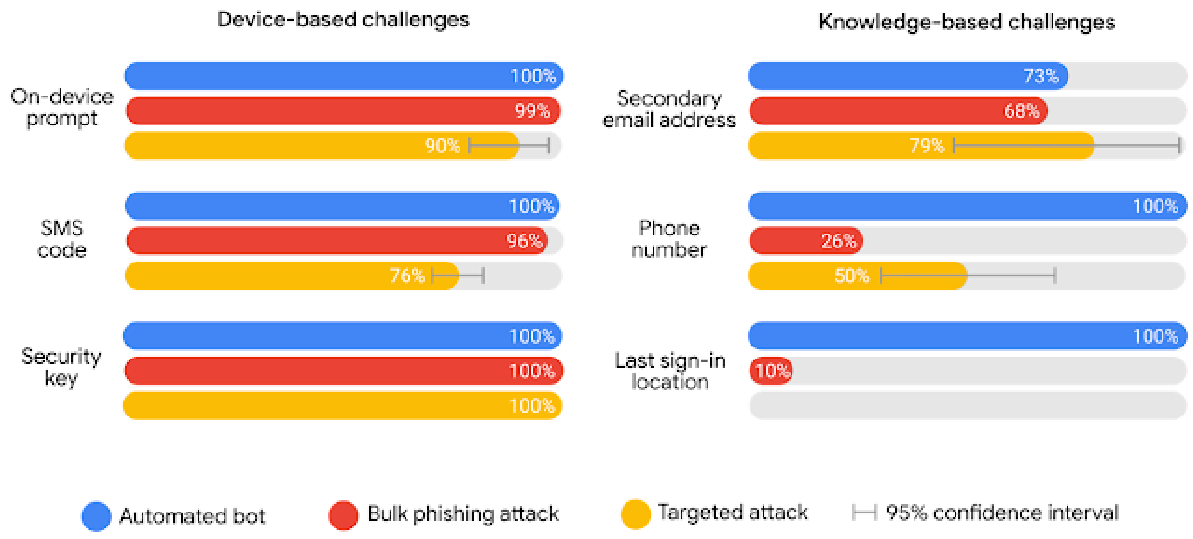
- Don’t be over confident
- Ensure that appropriate data protection and fund transfer protocols and training is in place – employees make mistakes
- Test and retest security measures and response scenarios – don’t underestimate the sophistication of cyber criminals
- Purchase cyber insurance!
- Encourage clients to keep backups on external servers
- Clients should also be testing backups are working

What can you be telling clients?

Loss mitigation continued...

- Recommend clients install multi-factor authentication

Account takeover prevention rates, by challenge type



Source: Google Security Blog 'New research: How effective is basic account hygiene at preventing hijacking,' 17.05.19 <https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html>

Questions