Deloitte.

Cyber Risk Services

Defensible incident management

Transforming Security Programs To Improve Resilience

Kevvie Fowler

February 2020

Cyber threat landscape

Cyber incident management

Q&A

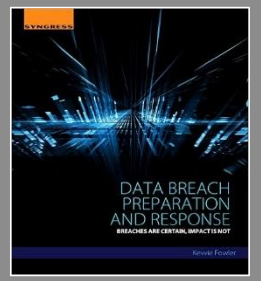
Kevvie Fowler

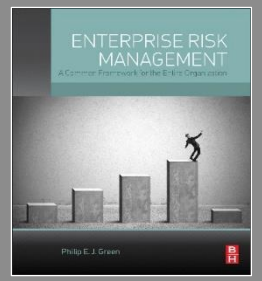
Partner, National Resilience Leader &
Global Incident Response Leader

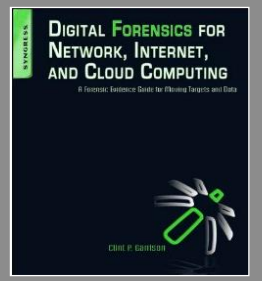
Career

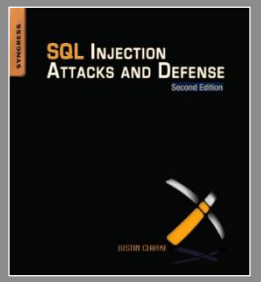
Other → Interac → BCE → TELUS → KPMG → **Deloitte**

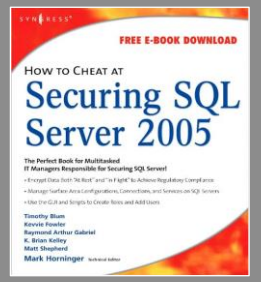
Books

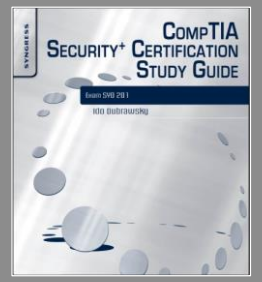












Certifications

- GCFA Gold
- CISSP
- SANS Lethal Forensicator
- MCTS, MCDBA, MCSD, MCSE

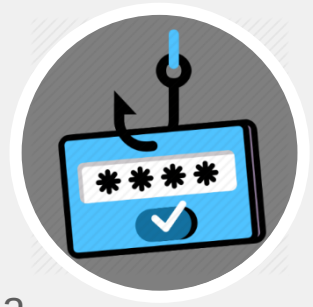
Selected Media

Deloitte.

Cyber threat landscape

The cyber threat landscape | a Canadian perspective

Phishing



47% of public sector cyber incidents occurred as a result of phishing

Ransomware

38% of public sector incidents were due to ransomware

11% of organizations paid the ransom

6 BTC was the average ransom request

Incidents by public sector area

47% affected municipalities

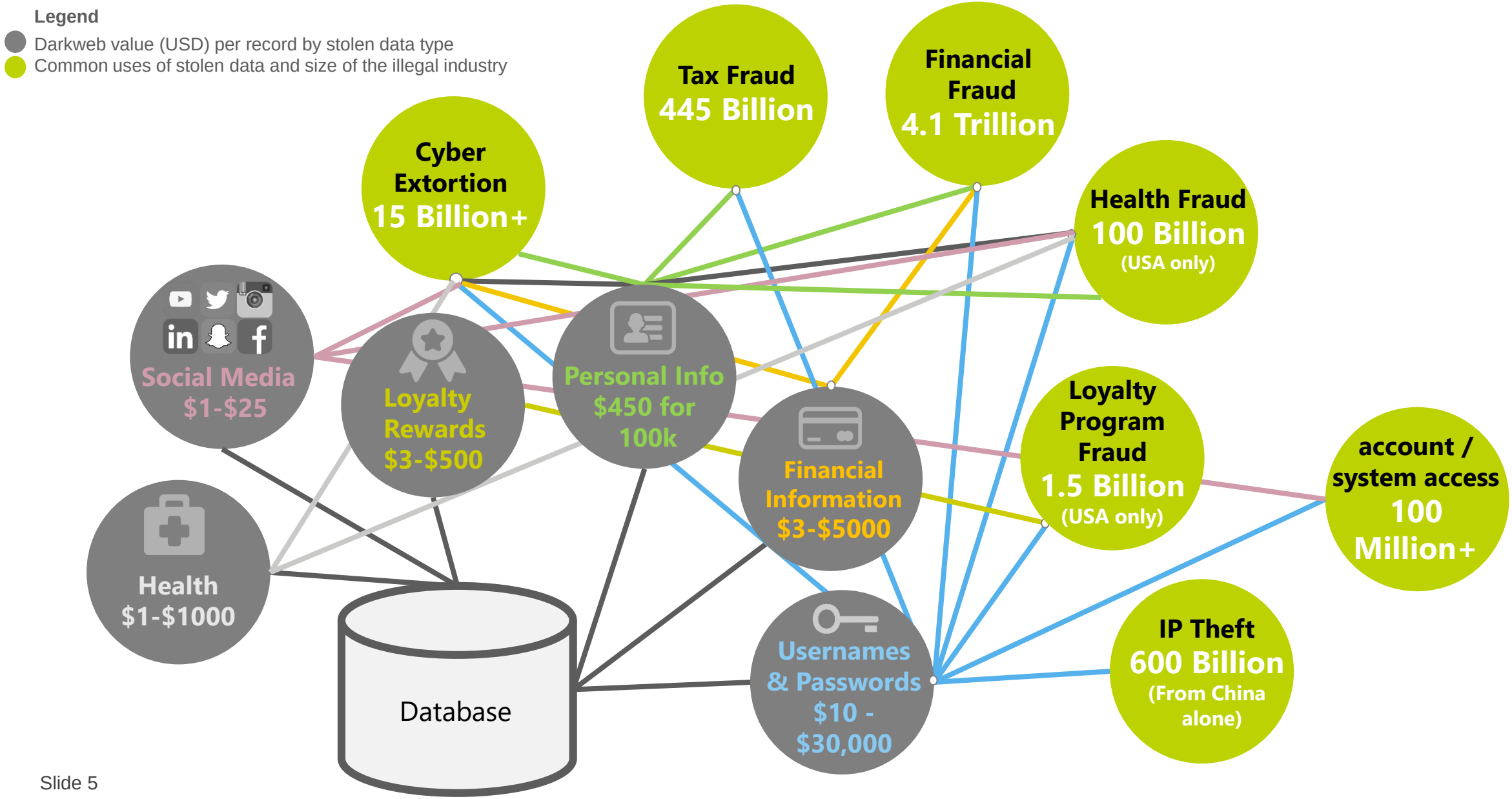
42% affected hospitals

11% affected social services

Notable threat actors

1. Orangeworm
2. APT41
3. Tropic Trooper
4. FIN4
5. menuPass
6. Stone Panda (APT 10, Red Apollo)
7. Deep Panda (Shell Crew, Kingfu Kittens)

The cyber threat landscape | Targeted data



Incident management

Incident management | Defensible response

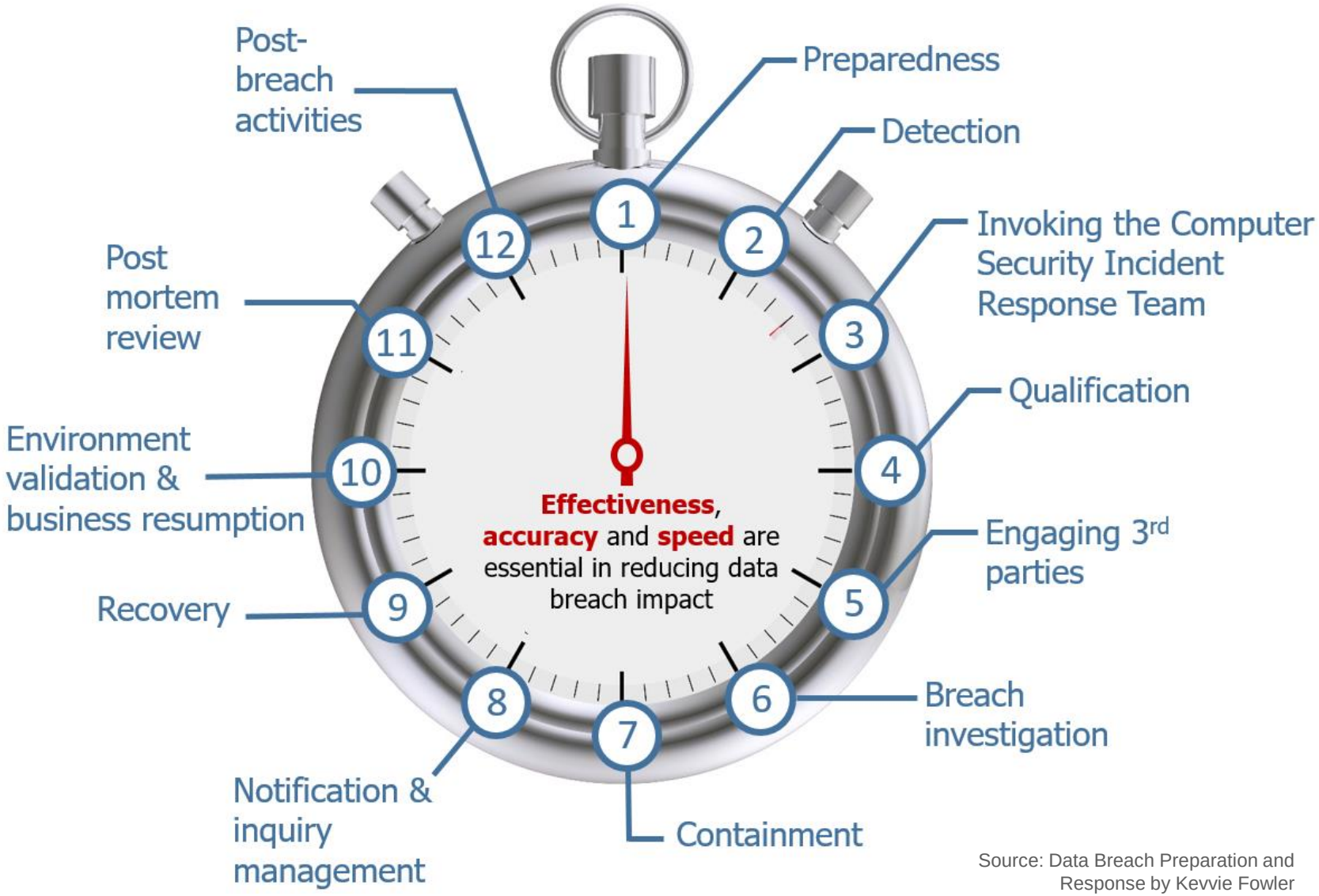
GDPR & PIPEDA

place expectations on many Canadian organizations to log and report on breaches in as little as **72** hours.

Incident metrics:

- **68%** Initial attack to compromise **within minutes***
- **56%** undiscovered for **months or more****
- **40%** containment required **weeks or longer****

** Verizon DBIR 2019



Source: Data Breach Preparation and Response by Kevvie Fowler

Incident management | Proactively protecting your organization

Effective cyber response is the last line of protection for your organization

Review and update you incident response program to ensure it is effective against incidents relevant to your organization

Run crisis simulations to assist in the operationalization and improve the effectiveness of your incident/crisis management program

Perform a compromise assessment to help test the effectiveness of your security program and ensure timely detection of incidents

Ensure defensible incident response to help ensure the effective management of an incident in a manner that reduces operational, financial and reputational impact

Run post-mortem reviews after an incident to identify what went well and lessons learned

Questions

Contact

Kevvie Fowler

Partner, National Resilience Leader &
Global Incident Response Leader
Tel: (905) 767-8067
Email: kfowler@deloitte.ca

Deloitte.