Defensible incident management
Transforming Security Programs To Improve Resilience

Kevvie Fowler
February 2020
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
- 6 BTC was the average ransom request
- 11% of organizations paid the ransom

**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

Legend:
- Darkweb value (USD) per record by stolen data type
- Common uses of stolen data and size of the illegal industry

- **Cyber Extortion** 15 Billion+
- **Tax Fraud** 445 Billion
- **Financial Fraud** 4.1 Trillion
- **Health Fraud** 100 Billion (USA only)
- **Loyalty Program Fraud** 1.5 Billion (USA only)
- **IP Theft** 600 Billion (From China alone)
- **Usernames & Passwords** $10 - $30,000
- **Financial Information** $3 - $5000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Health** $1 - $1000

Database

- **account / system access** 100 Million+
- **Health** $1 - $1000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

- **Tax Fraud** 445 Billion
- **Financial Fraud** 4.1 Trillion
- **Health Fraud** 100 Billion (USA only)
- **Loyalty Program Fraud** 1.5 Billion (USA only)
- **IP Theft** 600 Billion (From China alone)
- **Usernames & Passwords** $10 - $30,000
- **Financial Information** $3 - $5000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

100 Million+ account / system access

- **Health** $1 - $1000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

- **Tax Fraud** 445 Billion
- **Financial Fraud** 4.1 Trillion
- **Health Fraud** 100 Billion (USA only)
- **Loyalty Program Fraud** 1.5 Billion (USA only)
- **IP Theft** 600 Billion (From China alone)
- **Usernames & Passwords** $10 - $30,000
- **Financial Information** $3 - $5000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

100 Million+ account / system access

- **Health** $1 - $1000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

- **Tax Fraud** 445 Billion
- **Financial Fraud** 4.1 Trillion
- **Health Fraud** 100 Billion (USA only)
- **Loyalty Program Fraud** 1.5 Billion (USA only)
- **IP Theft** 600 Billion (From China alone)
- **Usernames & Passwords** $10 - $30,000
- **Financial Information** $3 - $5000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

100 Million+ account / system access

- **Health** $1 - $1000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

- **Tax Fraud** 445 Billion
- **Financial Fraud** 4.1 Trillion
- **Health Fraud** 100 Billion (USA only)
- **Loyalty Program Fraud** 1.5 Billion (USA only)
- **IP Theft** 600 Billion (From China alone)
- **Usernames & Passwords** $10 - $30,000
- **Financial Information** $3 - $5000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

100 Million+ account / system access

- **Health** $1 - $1000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

- **Tax Fraud** 445 Billion
- **Financial Fraud** 4.1 Trillion
- **Health Fraud** 100 Billion (USA only)
- **Loyalty Program Fraud** 1.5 Billion (USA only)
- **IP Theft** 600 Billion (From China alone)
- **Usernames & Passwords** $10 - $30,000
- **Financial Information** $3 - $5000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

100 Million+ account / system access

- **Health** $1 - $1000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

- **Tax Fraud** 445 Billion
- **Financial Fraud** 4.1 Trillion
- **Health Fraud** 100 Billion (USA only)
- **Loyalty Program Fraud** 1.5 Billion (USA only)
- **IP Theft** 600 Billion (From China alone)
- **Usernames & Passwords** $10 - $30,000
- **Financial Information** $3 - $5000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

100 Million+ account / system access

- **Health** $1 - $1000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

- **Tax Fraud** 445 Billion
- **Financial Fraud** 4.1 Trillion
- **Health Fraud** 100 Billion (USA only)
- **Loyalty Program Fraud** 1.5 Billion (USA only)
- **IP Theft** 600 Billion (From China alone)
- **Usernames & Passwords** $10 - $30,000
- **Financial Information** $3 - $5000
- **Personal Info** $450 for 100k
- **Loyalty Rewards** $3 - $500
- **Social Media** $1 - $25
- **Database**

100 Million+ account / system access
Incident management
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***

' Source: Data Breach Preparation and Response by Kevvie Fowler

** Post-mortem review

** Environment validation & business resumption

** Recovery

** Notification & inquiry management

** Preparedness

** Detection

** Invoking the Computer Security Incident Response Team

** Qualification

** Engaging 3rd parties

** Breach investigation

** Containment

** Effectiveness, accuracy and speed are essential in reducing data breach impact

' ** Verizon DBIR 2019

Source: Data Breach Preparation and Response by Kevvie Fowler
Effective cyber response is the last line of protection for your organization

- **Review and update your 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, one of Canada’s leading professional services firms, provides audit, tax, consulting, and financial advisory services. Deloitte LLP, an Ontario limited liability partnership, is the Canadian member firm of Deloitte Touche Tohmatsu Limited.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

The information contained herein is not intended to substitute for competent professional advice.

© Deloitte LLP and affiliated entities.