RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: AIR-R02

How CTI Can Play a Key Role to Get Security on Board

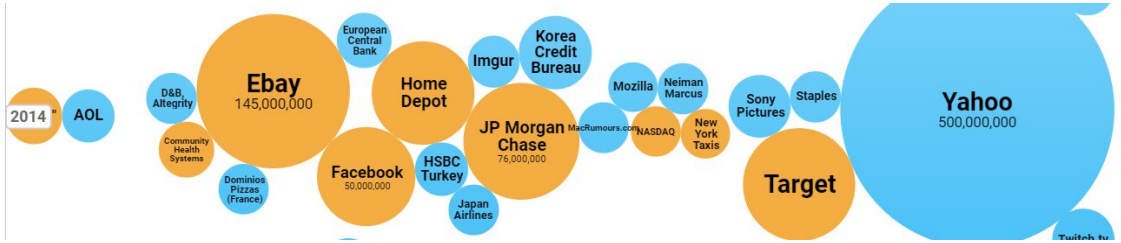
Jean-Yves Riverin

Cyber Threat Intelligence Senior Advisor
Desjardins Group
@JYRiverin

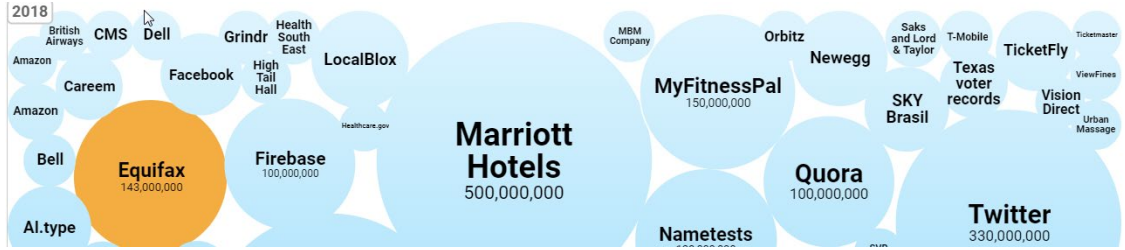
Was it easier to be in the security fields 5 years ago?

World's Biggest Data Breaches & Hacks

2014



2018



A few examples

amazon.com

#cloudbleed

AdultFriendFinder

EQUIFAX

WannaCry
Ransomware Attack

SWIFT

Globality of the new economy

Execs wants to know

RSAConference2019

Our tasks

Sources, Methods, Analysis, Actionnable, Communications

Our tasks

- Define PIR (Priority Intelligence Requirements)
  - Questions that allow threat intelligence personnel to focus on what is important to the operator and management.
- Sources
  - OSINT (Open-source intelligence), HUMINT (Human Intelligence), Peers, Digital footprint, Scanners
- Methods
  - Automatisation, TIP (Threat Intelligence Platform)
- Analysis
  - Inventory, tools, etc.
- Actionnable
  - TIP, automatisation, Triage, etc.
- Communications
  - Alerting, portal, Mobile app for Execs, etc.

Our tasks - Sources

- Internal data
  - CMDB (configuration management db) , SIEM (Security Event Information Management), Projects
- OSINT
  - Twitter
  - Mailing lists
  - Subscriptions (Abuse.ch, Shodan, etc)
  - DFIR (Digital Forensics and Incident Response)
- HUMINT
  - Various sectors
- Peers
  - Banks, ISAC (Information Sharing and Analysis Center), Governments
- Digital footprint, scanners
  - VRM (Vendor Risk Management), DRM (Digital Risk Management)
- Paid threat intel feeds

Our tasks - Methods

- Automatisation
  - Various scripts (Github)
- TIP
  - Threat Intelligence Platform
    - Aggregation
    - Single repository for SIEM
    - Share with peers

Our tasks - Analysis

- Inventory
  - Assets
  - Scans
  - Projects
- Tools
  - CMDB
  - Domain monitoring
  - LinkedIn
  - Portal
- etc.

Our tasks - Actionnable

- TIP
  - IOC ingestion (Indicator of compromise)
  - Connected to our SIEM (Degree of confidence)
- Automatisation
  - Useful to pre-analyze data based on keywords
  - Generate emails
  - Pre-filtering for communications

Our tasks - Communications

- Alerting
- CTI Portal
- Mobile app for Execs
- Monthly, Weekly, Ad-hoc documents
- Briefing (Operational, Execs)
- Road show
- etc.

RSAConference2019

Steps we have done

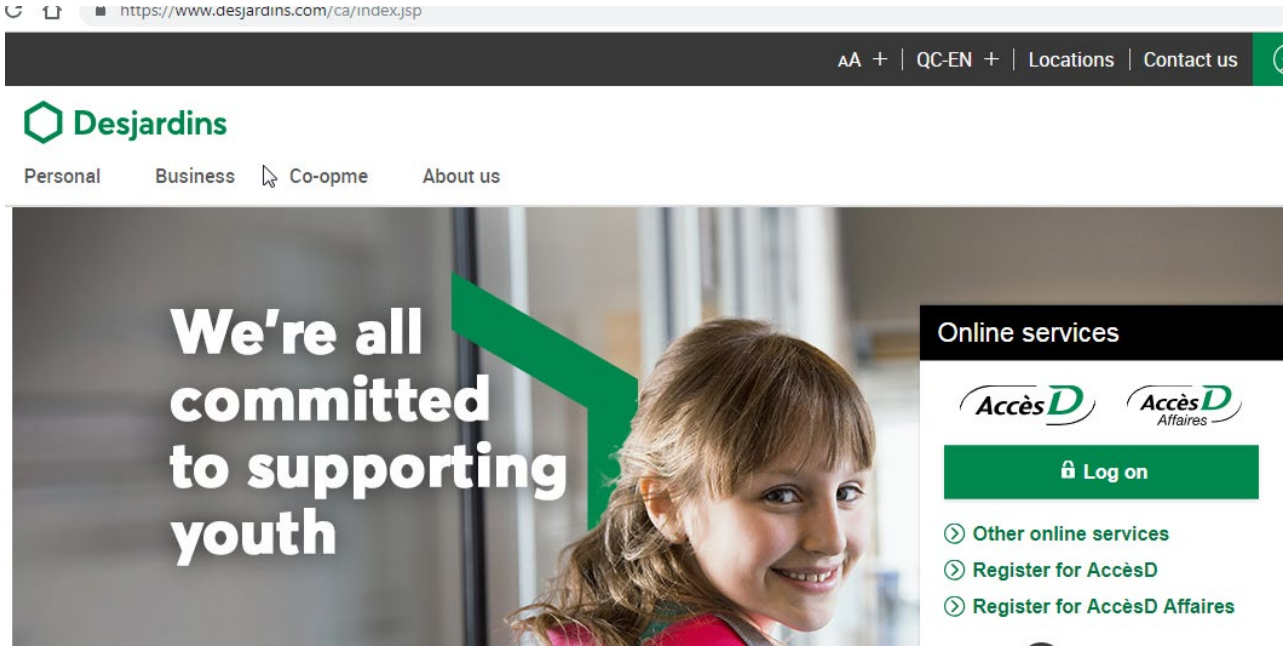
Know everything about anything…

Steps we have done

- Know your own company
- Know your org chart
- Know your crown jewels
- Share with partners
- Communications
- Be passionate!

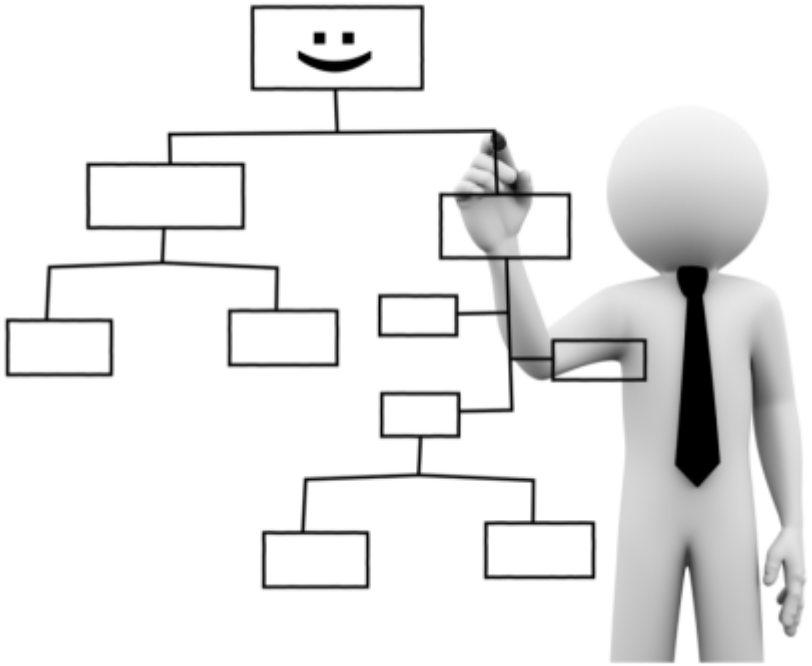
Steps we have done

- Know your own company



Steps we have done

- Know your Organizational chart



Steps we have done

- Know your crown jewels

Steps we have done

- Share with partners

Gouvernement du Canada

TWITTER

Échange Canadien De Menaces Cybernétiques
Informer les entreprises canadiennes

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

H-ISAC™
HEALTH - ISAC

FINANCIAL SERVICES Information Sharing and Analysis Center

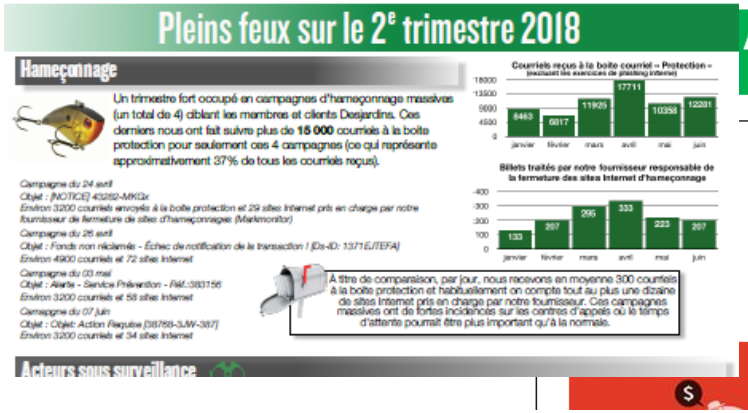
CANADIAN CENTRE FOR CYBER SECURITY | CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

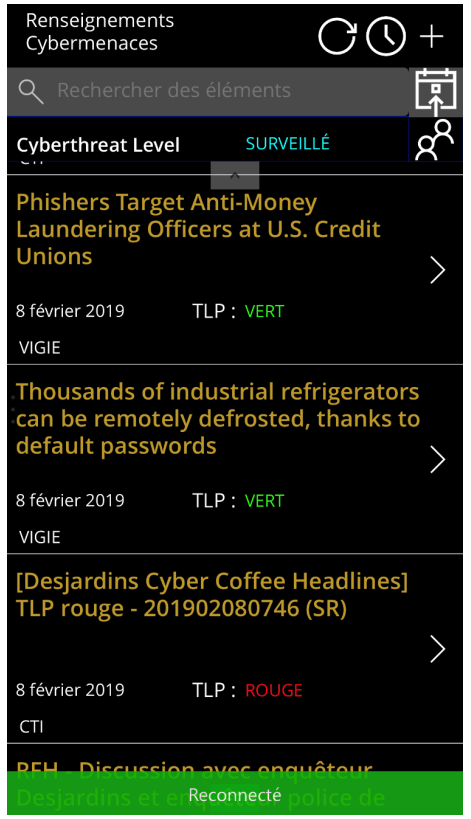
Royal Canadian Mounted Police | Gendarmerie royale du Canada

Desjardins

Communications

- Monthly, Weekly, Ad-hoc





Steps we have done

- Be passionate!

RSAConference2019

Now, what can I do?

Apply What You Have Learned Today

- Next week you should:
  - Know your company a little bit better. Lots of information already around you.
    - Browse your company's website/Social media
    - Identify all the sector of activities of your company
    - Identify 10 partners (Ex: Clients, providers)
  - Know your org chart
    - CISO, Executives, IT team, SOC, Business units, (If applicable)
  - Know your crown jewels
    - What is your value as a company?
    - What can be your greatest risks?
    - Who can be your attackers? (Nation states, Script kiddies, etc.)
    - What can be their motives? (Profits, disrupt, etc.)

Apply What You Have Learned Today

- In the first three months following this presentation you should:
  - Have a clear view of you company, subsidiaries
  - High level pictures of your org chart, relationships (who's who)
  - Understand your biggest current cybersecurity threats based on your sector of activities
  - Make "new friends" in all your lines of businesses
  - Have made 3 PIR concerning your company

Apply What You Have Learned Today

- Within six months you should:
  - Set up a Cyber Threat Intelligence practice (Roles and Responsibilities)
  - Identify and acquire different sources of information related to your PIR (OSINT at first)
  - Organize and store Threat Information (Even in a spreadsheet)
  - Distribute Threat Intelligence internally (By email at first)
  - Consume Threat Intelligence in your monitoring tools (SIEM)

RSAConference2019

Are we successful?

Is our CTI program successful?

- Incidents
  - From reactivity to proactivity
- External audits
  - Maturity level
- Involvements in projects/Questions from business units
  - We are advised before
- Invitations to various forums (Internal, External, C-Level committees)

Was it easier to be in the security fields 5 years ago?

RSAConference2019

Thank you!