

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: AIR-R02

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

Jean-Yves Riverin

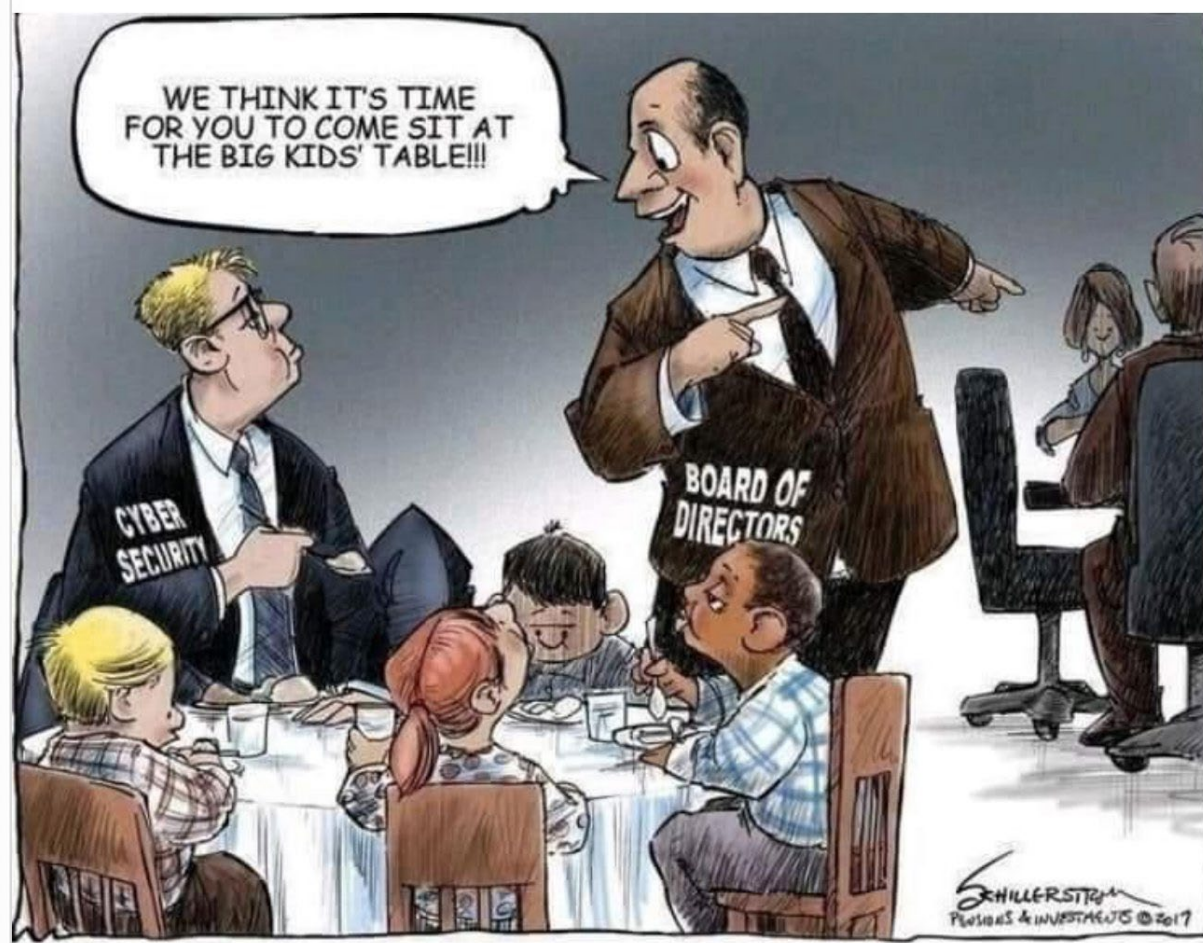
Cyber Threat Intelligence Senior Advisor
Desjardins Group
@JYRiverin



#RSAC

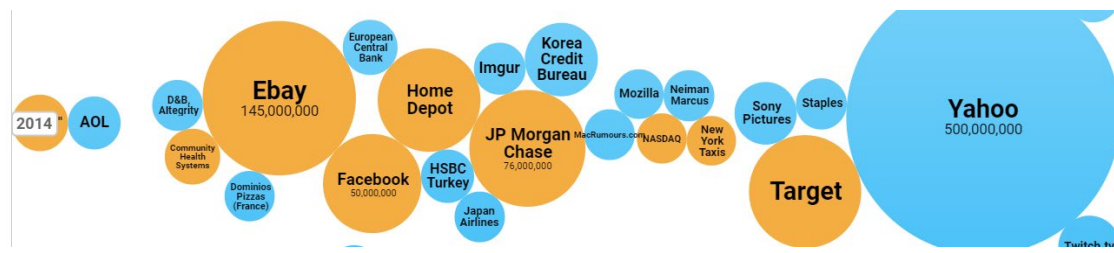
Was it easier to be in the security fields 5 years ago?

#RSAC

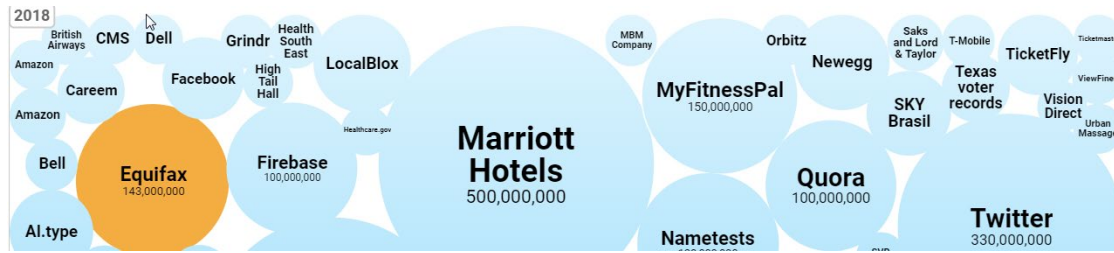


World's Biggest Data Breaches & Hacks

2014



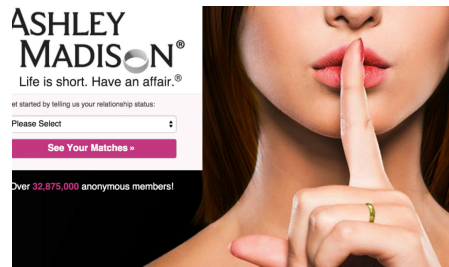
2018



A few examples



AdultFriendFinder



Globality of the new economy



Execs wants to know



RSA[®]Conference2019

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
 - Automatisations, TIP (Threat Intelligence Platform)
- Analysis
 - Inventory, tools, etc.
- Actionnable
 - TIP, automatisations, 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

- Automatisatisation
 - 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)
- Automatisatisation
 - Useful to pre-analyze data based on keywords
 - Generate emails
 - Pre-filtering for communications

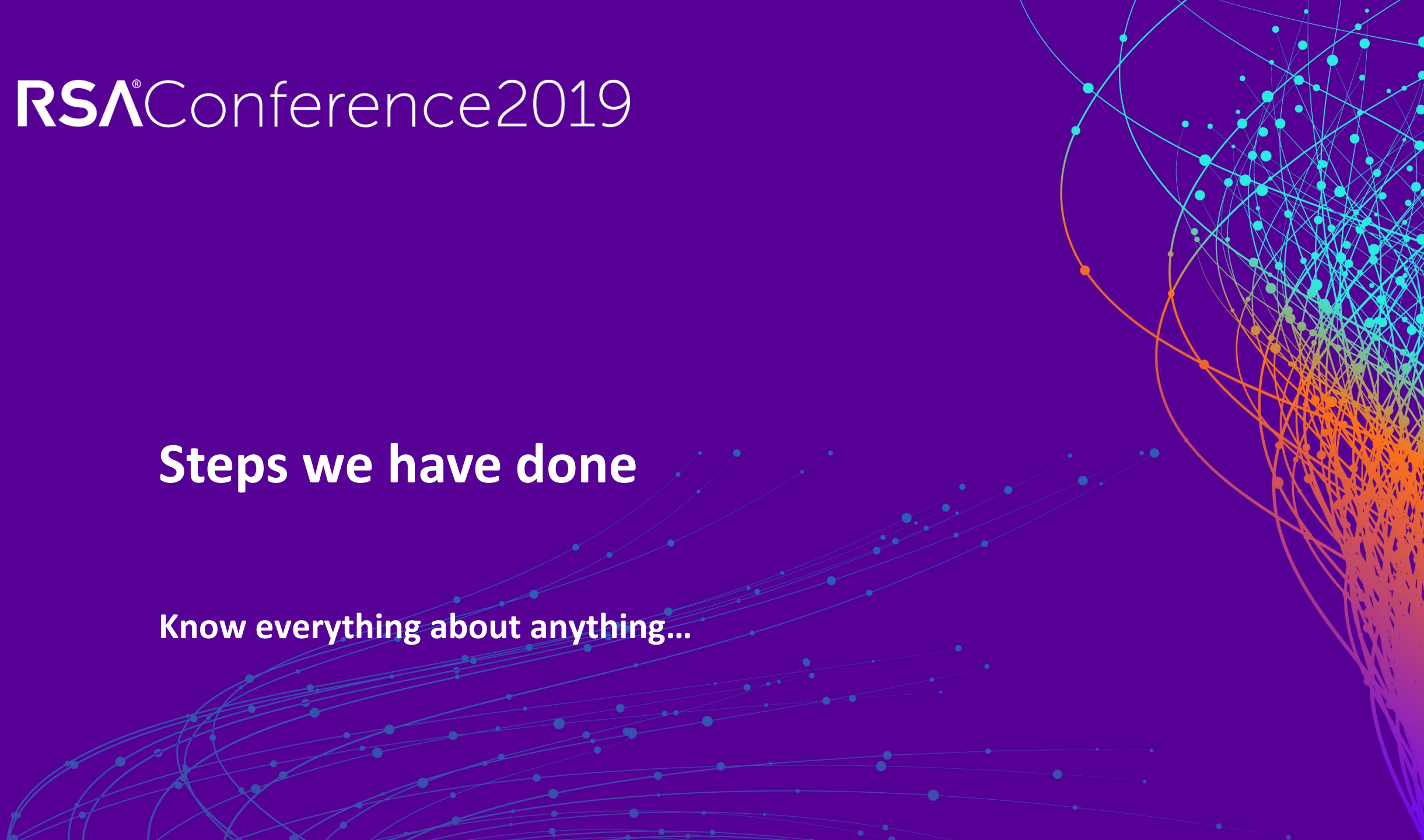
Our tasks - Communications

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

RSA[®]Conference2019

Steps we have done

Know everything about anything...

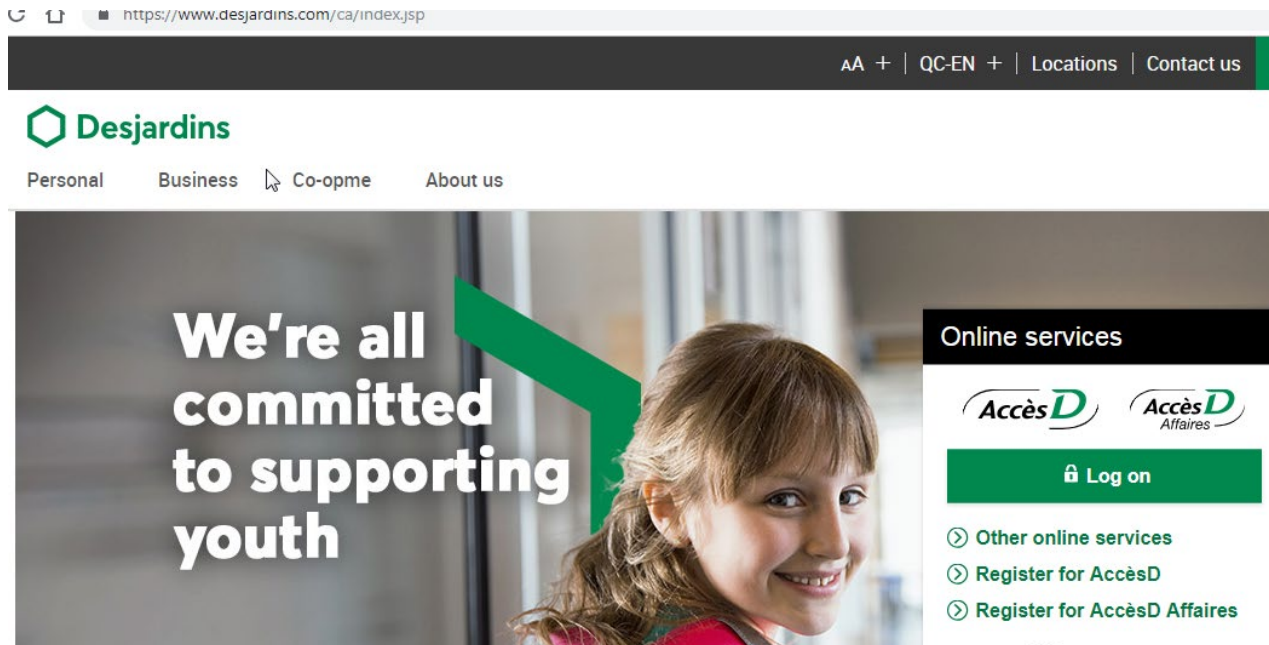


Steps we have done

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

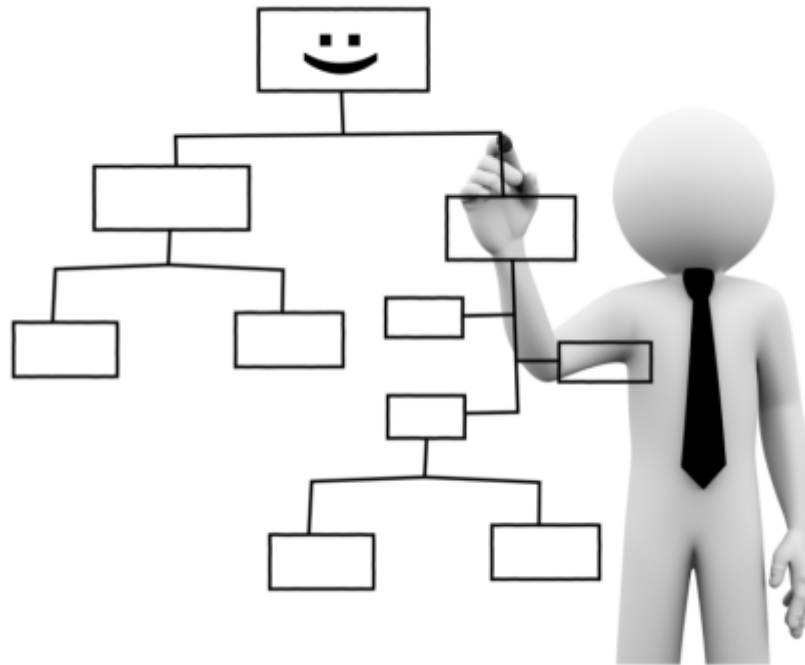
Steps we have done

- 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



Échange **Canadien**
De Menaces Cybernétiques
Informer les entreprises canadiennes

TWITTER



H-ISAC™
HEALTH - ISAC



**FINANCIAL
SERVICES** | Information
Sharing and
Analysis Center



CANADIAN CENTRE FOR
CYBER SECURITY | CENTRE CANADIEN POUR LA
CYBERSÉCURITÉ



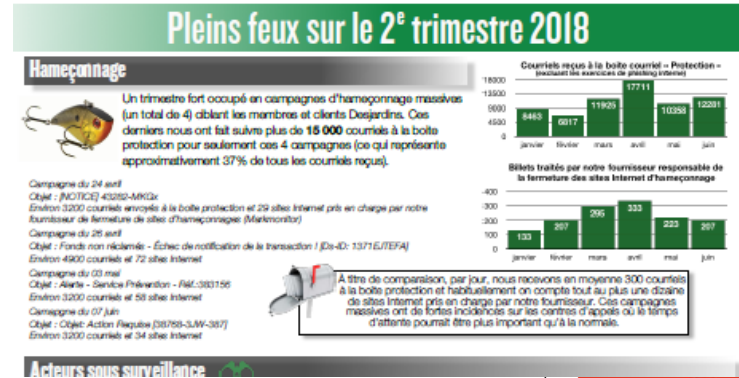
Royal Canadian
Mounted Police | Gendarmerie royale
du Canada

Communications

- Monthly, Weekly, Ad-hoc



CTI - CYBER THREAT INTELLIGENCE
D Intervention Tactique Sécurité | DP Risques et Sécurité de l'information



Actualité de la dernière semaine 22 au 28 juillet 2018

LabCorp victime d'une attaque par ransomware

LabCorp, l'un des plus grandes clinique laboratoires des États-Unis spécialisée dans les analyses de biologie médicale, a déclaré que l'attaque de Samsam ransomware qui a forcé leurs systèmes hors ligne a été contenue rapidement et n'a pas entraîné de violation de données. Cependant, dans le court laps de temps écoulé entre la détection et l'atténuation, le rançongiciel a pu chiffrer des milliers de systèmes et plusieurs centaines de serveurs de production.

L'attaque de Samsam à LabCorp a débuté à minuit le 13 juillet. C'est à ce moment-là que le groupe Samsam a utilisé une attaque de type

Renseignements
Cybermenaces

Rechercher des éléments

Cyberthreat Level **SURVEILLÉ**

Phishers Target Anti-Money Laundering Officers at U.S. Credit Unions

8 février 2019 TLP : VERT

VIGIE

Thousands of industrial refrigerators can be remotely defrosted, thanks to default passwords

8 février 2019 TLP : VERT

VIGIE

[Desjardins Cyber Coffee Headlines] TLP rouge - 201902080746 (SR)

8 février 2019 TLP : ROUGE

CTI

RFH - Discussion avec enquêteur Desjardins et e

Reconnecté police de

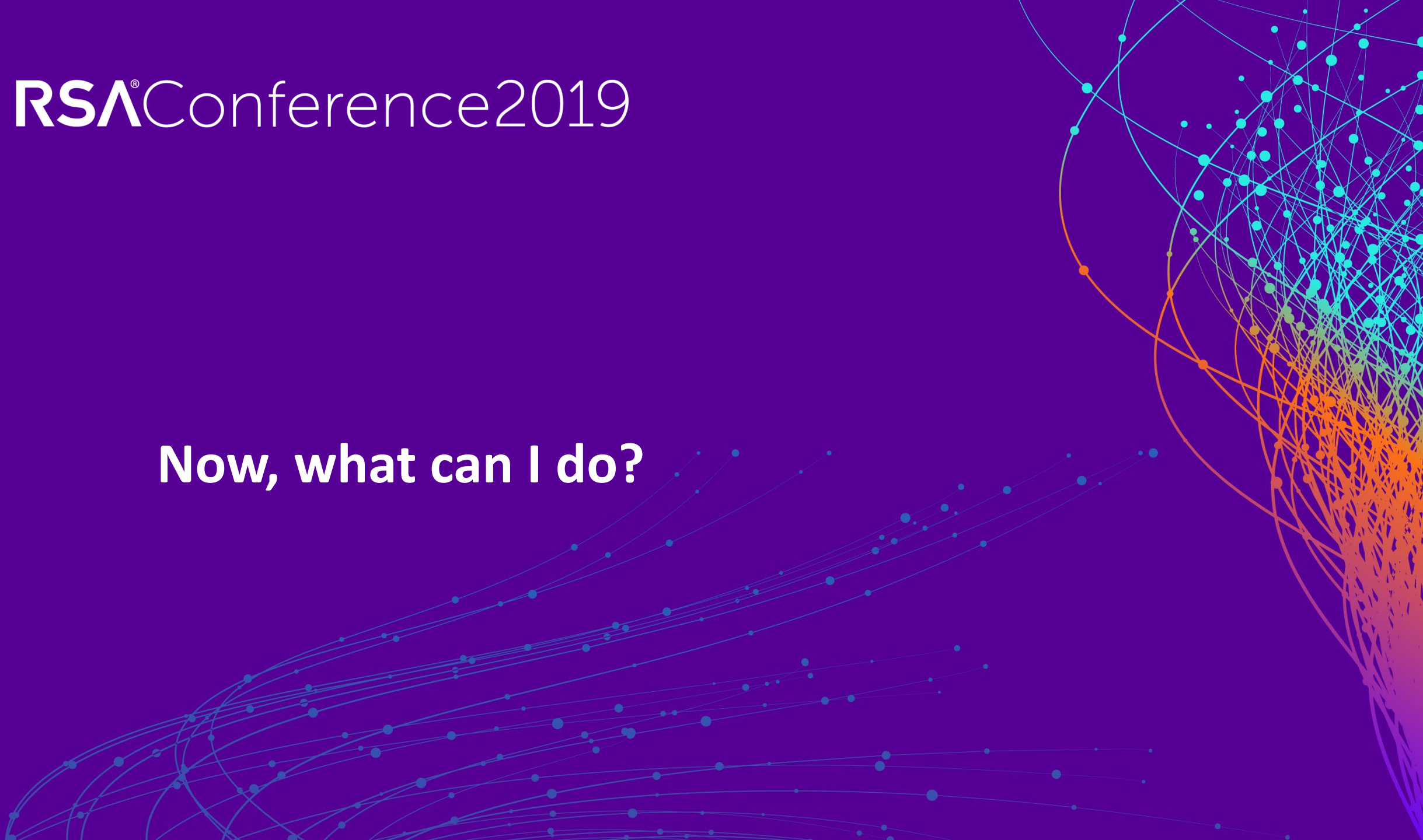
Steps we have done

- Be passionate!



RSA[®]Conference2019

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?

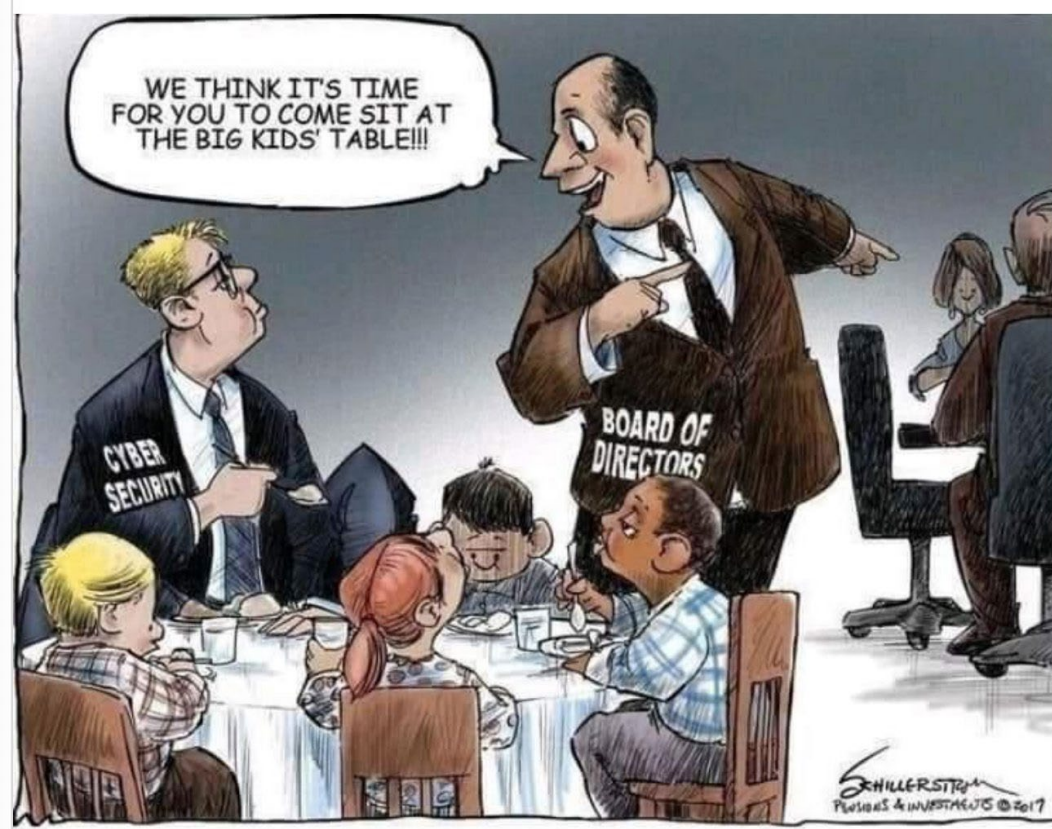


Is our CTI program successful?

- 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?

#RSAC



RSA®Conference2019

Thank you!

