Cyberattacks: Stakeholder & Responses, Impacts & Trends (Part 1)

La montée de la cybercriminalité : Quel est le coût réel? (Première Partie)

By/Par Thibault Dambrine

In this article, I will describe:

- Cyberattack response stakeholder roles and processes

In the next issue, I will describe:

- The impact cyberattacks have on organizations and people
- Risk mitigation investments, points of references and trends

Dans cet article, nous allons enquêter sur :

- Les rôles et processus des intervenants en matière de cyberattaques

Dans le prochain numéro, nous allons couvrir :

- L'impact des cyberattaques sur les organisations et les personnes
- Les investissements possibles pour atténuer les risques, ainsi que des points de référence

Risk mitigation investments, points of references and trends At the end of 2019, news of a distant epidemic by the name of "Covid-19" started making headlines. Within a few short weeks, it spread throughout the world. This laptop event triggered a global shift for knowledge workers. To help prevent the virus spread, those who could remain productive using a connected through the Internet were told to work from home.

For most organizations, having workers connect remotely via the Internet on casual basis or for support reasons had always been technically available. Very few organizations, however, were equipped with enough capacity to handle the increased volume required by workers connecting from home due to Covid-19. At that time, many organizations did not use multi-factor authentication (MFA) for external connectivity. Some opened Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC) ports as a temporary measure to accommodate the need for additional remote desktop sessions. This all happened quickly, at the cost of additional cyberattack risk.

In a parallel world, tech-savvy thieves did not fail to notice a massive opportunity. A cybercrime boom was born, complete with a surge in "Ransomware as a Service" (RaaS) attacks, a variation on the "Software as a Service" (SaaS) business model. The 2021 FBI Internet Crime Report shows that between 2019 and 2020 alone, the number of cybersecurity complaints increased by almost 70%.

Today, cybercrimes openly reported in the news are no longer unusual events. What has changed however is that such attacks tend to affect larger number of individuals, stranding airline passengers, causing gasoline shortages,

Vers la fin de 2019, une nouvelle épidémie lointaine a commencé à faire les gros titres dans les nouvelles. En quelques semaines, la Covid-19 s'est répandue dans le monde entier. Pour aider à prévenir la propagation du virus, beaucoup ont été encouragés à travailler depuis leur domicile, via l'Internet.

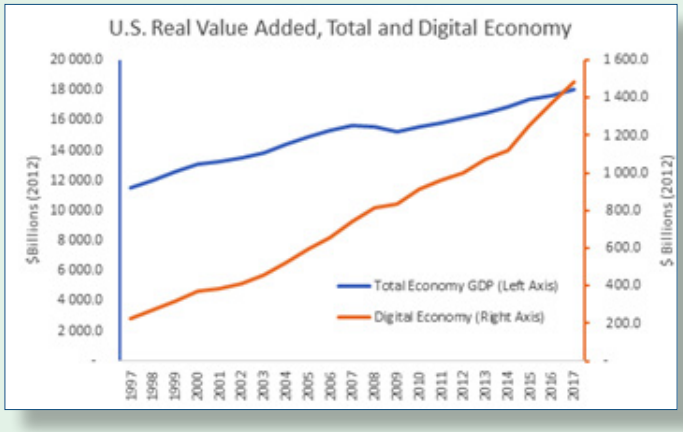
Pour la plupart des organisations, avoir un nombre limité de travailleurs connectés à distance via Internet de manière occasionnelle, ou pour des raisons de soutien, était techniquement établi. Peu d'organisations, cependant, étaient équipées de capacité suffisante pour gérer le volume accru requis pour les travailleurs se connectant depuis leurs domiciles en raison de la Covid-19. De nombreuses organisations n'utilisaient pas l'authentification multi facteur (« multifactor authentication » ou MFA) pour la connectivité externe. Une solution « à court terme » souvent utilisée pour résoudre rapidement ce problème de capacité consistait à ouvrir des ports dits de « bureau à distance » (Remote Desktop Protocol RDP) ou VNC (Virtual Network Computing) comme mesure temporaire, pour répondre au besoin de sessions bureau à distance supplémentaires. En mettant ces mesures en œuvre en urgence, de nombreuses organisations ont augmenté leur risque d'exposition aux cyberattaques.

Les cybercriminels n'ont pas manqué de remarquer une énorme opportunité. Un boom de la cybercriminalité est né, et avec elle, une recrudescence d'attaques a partir de « rançongiciel comme service » ou de « Ransomware as a Service » (RaaS), une variante du modèle économique « Software as a Service » (SaaS). Le FBI Internet Crime Report 2021 montre qu'entre 2019 et 2020 seulement, le nombre de plaintes en matière de cybersécurité a augmenté de près de 70% aux États- Unis. Le reste du monde n'a pas été épargné.

leaking banking customer data, crippling hospitals and more. The damage is real, it is visible, it is far-reaching and it affects people's lives. This is not a "victimless crime".

Part 1: Cyberattack Stakeholders & Responses

The chart below shows how quickly digital transactions have changed our lives. As a result, the value of the data within has increased significantly. Despite its increased value, data, stored locally, on the Cloud or in movement, remains vulnerable. It must be backed up, protected and constantly monitored for possible corruption. It must be, but is it? Cyberthieves have noticed the vulnerabilities.



Source: https://www.nist.gov/blogs/taking-measure/cybercrime-its-worse-we-thought

The target, in any Cyberattack, is data. At first glance, this appears to be a technical issue, with technical solutions. There are in fact three key additional implications and technical recovery is part of that set. Here is the bigger picture:

1) Legal Considerations:

- In Canada, the Personal Information Protection and Electronic Document Act (PIPEDA), mandates reporting breaches where personal information may put individuals at risk.
- As custodian of sensitive client information, a company or organization that is hacked or breached with a cyberattack may be subject to lawsuits from customers, joint-venture partners and other outside stakeholders who were counting on their data to be properly secured.

2) Insurance considerations:

- Data, in digital form, has become so integral to most company functions that it is now considered an asset.
  - o Companies, organizations, protect their assets against risk with insurance policies. Buildings and vehicles come to mind. Data, either in motion (think of e-commerce, process control systems) or in storage (think of HR personnel information), is also a working asset which warrants protection.
  - o Insurance companies assess the risk and charge

Aujourd'hui, les cybercrimes ouvertement rapportés dans les nouvelles ne sont plus des événements inhabituels. Ce qui a changé, c'est que de telles attaques ont tendance à affecter un plus grand nombre de personnes, bloquant les passagers de lignes aériennes dans les aéroports, provoquant des pénuries d'essence, divulguant des données sur les dépositaires bancaires, paralysant les hôpitaux et plus encore. Les dégâts sont réels. Ils sont visibles. Ils sont d'une grande portée. Ces crimes affectent la vie des gens. Contrairement a ce que l'on entend trop souvent, ce ne sont pas des « crimes sans victimes ».

Première Partie : Intervenants et réponses aux cyberattaques

Le graphique à gauche montre à quelle vitesse les transactions numériques ont changé nos vies. En conséquence, la quantité de données que nous partageons personnellement avec les organisations a augmenté et la valeur de ces données a également augmenté de manière significative.

Malgré leur valeur accrue, les données, stockées localement, sur le Cloud ou en mouvements, qui ne sont pas protégées de manière adéquate restent vulnérables aux cybercriminels. Dans cet esprit, les entreprises et les organisations doivent s'assurer qu'elles sont sauvegardées, protégées et constamment surveillées pour détecter d'éventuelles corruptions.

Le graphique à gauche reflète la vitesse a laquelle la valeur de l'économie digitale (courbe orange) a augmenté, par rapport à l'économie traditionnelle (courbe bleue)

La cible, dans toute cyberattaque, ce sont les données. À première vue, une cyberattaque peut sembler être un problème technique, avec des solutions techniques. Il y a en fait trois implications additionnelles. L'aspect technique n'est qu'une partie de cet ensemble. Voici une vue d'ensemble :

1) Considérations relatives aux coûts :

- Implications de l'interruption d'activité - en 2022, le délai moyen entre le chiffrement et la récupération complète du système est d'un mois (voir lien)
- Le coût de la récupération des données et des systèmes – la récupération technique que nous avons décrite précédemment
- Le temps nécessaire pour reconstruire les relations clients existantes
- Le coût supplémentaire de convaincre de nouveaux clients de faire des affaires, après une cyberattaque réussie
- Le coût du paiement de la rançon, si un ransomware et/ou l'extraction de données est impliqué

2) Considérations relatives à l'assurance :

- Les données, sous forme numérique, sont devenues si intégrées à la plupart des fonctions de l'entreprise qu'elles sont maintenant considérées comme un « actif », au sens comptable.
  - o Quand on pense à «la protection des actifs »,

premiums for individual types of coverage. Insurance policies aimed at protecting data from the risk of cyberattacks are one of those.

- If a company has a cyber insurance policy at the time when they get hacked, the insurer will no doubt be called and get involved. There is good reason to have data insured. Cyberattack damages can be very expensive.

3) Cost Considerations:

- The cost of ransoms, if ransomware or data extraction is involved
- The cost of not being able to do business - in 2021, the average time from encryption to full system recovery is one month. (Source: https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/)
- The cost of recovering data and systems – the technical recovery we described earlier on
- The cost of regaining confidence from existing customers
- The additional cost of convincing new customers to do business, after a successful cyberattack

Imagine being an IT manager, coming to work on a Monday morning following a long weekend. The first thing you find out that all the systems you are responsible for are no longer operational. One of the server console screens shows a note describing the terms of a ransom. What's next?

Business is halted. The phone is ringing. There is a sense of urgency to get things fixed quickly. Cyberattack recovery is intricate by nature. Data may be encrypted. It may be compromised. Backup data may be affected as well. Data may have been extracted by the hackers. Applications may no longer be operational. Operating systems may be impacted or modified with back-door access points. HR and personnel data, such as SIN numbers, may be at risk. On minute one, there is no estimated time for recovery. Understanding the extent of the damage takes time. This is a high-stress situation. Data has been leaked, destroyed, altered, or made unusable on your watch.

What type of attacks are we talking about? How do hackers get started? What type of damage do they cause? The following graph provides an overview of entry points and attack methods:

In this scenario, we made the assumption is that the organization has cyber insurance coverage. Once past the initial shock, as the IT manager, you will lead that first phone call to the insurer. The following paragraphs will describe what you may be able to expect past that point. As a start, the insurance company will recommend using two distinct services:

1) The immediate technical emergency is a prime concern. A recommendation will be made to hire trusted a third-party

les entreprises, les organisations, protègent leurs actifs contre les risques avec des polices d'assurance. Les bâtiments et les véhicules viennent à l'esprit. Les données sont aussi considérées comme des actifs, qu'elles soient

- En mouvement (pensez au commerce électronique, aux systèmes de contrôle des processus)
- Stockées (pensez aux informations sur le personnel des RH) sont également des actifs fonctionnels qui méritent d'être protégés.

o Pour facturer d'une façon appropriée les primes d'assurance pour différents types d'actif et de couverture, les compagnies d'assurance évaluent les risques. Les polices d'assurance visant à protéger les données contre les risques de cyberattaques font partie de cet ensemble de méthodes.

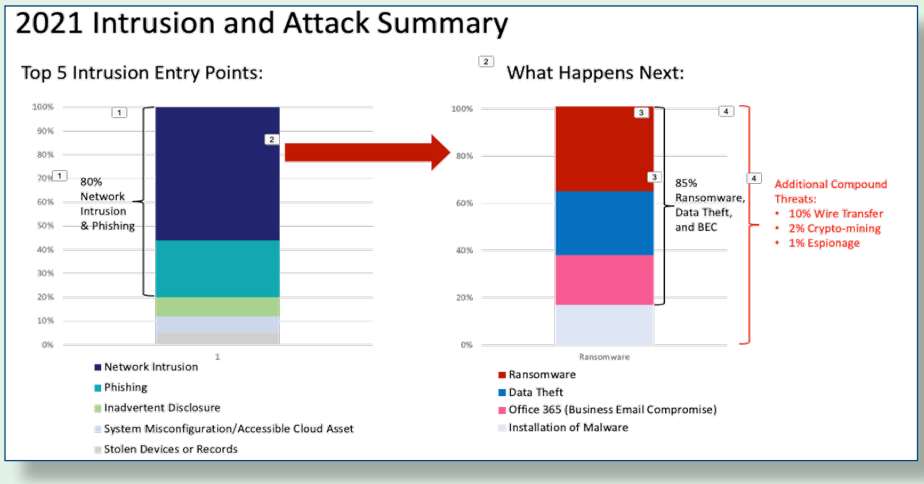
- En cas d'attaque, si une entreprise détient une police d'assurance pour la cybersécurité, la première étape logique consiste à initier une réclamation sur cet incident contre la police.
  - o Les compagnies d'assurances ont typiquement un nombre de contacts professionnels et experts à leur disposition dans leurs carnets de ressources. Avec cet aide, ils peuvent aider leurs clients à se remettre en ligne plus rapidement, réduire le risque de problèmes juridiques et dans certains cas, gérer les relations de presse autour de l'incident.

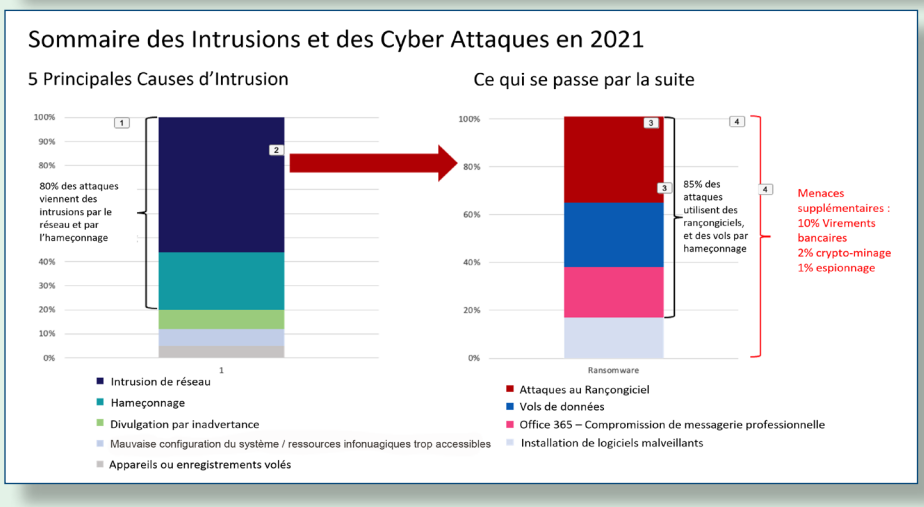
3) Considérations juridiques :

- Au Canada, la Loi sur la protection des renseignements personnels et les documents électroniques (Personal Information Protection and Electronic Document Act - PIPEDA) exige le signalement des atteintes à la protection des renseignements personnels lorsque des renseignements personnels peuvent mettre les personnes en danger.
- Un dépositaire d'informations sensibles sur les clients, une entreprise ou une organisation piratée ou violée par une cyberattaque peut faire l'objet de poursuites de la part de clients, de partenaires de coentreprise et d'autres parties prenantes externes qui comptaient sur la sécurité de leurs données.

Imaginez d'être un responsable d'un département d'informatique. Vous venez travailler un lundi matin. La première chose que vous découvrez, c'est que tous les systèmes dont vous êtes responsable ne sont plus opérationnels. L'un des écrans de la console du serveur affiche une note décrivant les conditions d'une rançon. Quelle est la prochaine étape?

Les affaires sont arrêtées. Les téléphones sonnent de partout. Il y a un sentiment d'urgence à régler les choses rapidement. La récupération des cyberattaques est





cybersecurity consulting company with one or more the following capabilities, depending on the specific requirements:

- Data and system recovery experts
- Ransomware negotiation experience
- Digital forensic experts
- Cybersecurity specialists

Trust, experience and proven competence are key factors in this choice.

2) To coordinate the recovery, which is almost invariably complex, a breach coach will be assigned. The breach coach is almost always a lawyer. This is to address the foreseeable legal issues to come, after a cyberattack, in effect providing both the coaching advice and the legal counsel.

One of the most common risks resulting from a cyberattack is that personal identifiable information (PII) or personal health information (PHI) may be divulged. In addition, confidential corporate data, such as patents or company secrets may be at risk as well. The role of the breach coach is to guide the organization in identifying the requirements related to data privacy and help advise on retaining a competent, trusted third-party providers to help control and contain post attack damage.

These include:

- Hiring credit monitoring services
- Advising on public relation strategies and specialists
- Ensuring post breach obligations are satisfied for each of the jurisdictions that the company operates in, as well as the implications.
- In many cases, advise on the decision of what technical recovery service (mentioned in point 1 above) companies may be used.

complexe par nature. Les données peuvent être chiffrées, elles peuvent être compromises et les données de sauvegarde peuvent également être affectées. Des données peuvent avoir été extraites par les pirates. Les applications peuvent ne plus être opérationnelles. Les systèmes d'exploitation peuvent être affectés ou modifiés avec des points d'accès dérobés. Les données sur les RH et le personnel, comme les numéros d'Assurance Sociale ou de compte bancaire, peuvent être à risque.

À la première minute, il n'y a pas de temps estimé pour la récupération. Comprendre l'étendue des dégâts prend du temps. Il s'agit d'une situation typiquement très stressante. Des données sensibles peuvent avoir été volées, divulguées, détruites, modifiées ou rendues inutilisables sous votre gouverne.

De quel type d'attaques parle-t-on ? Comment les pirates informatiques commencent-ils? Quel type de dommages causent-ils? Le graphique suivant fournit une vue d'ensemble des points d'entrée et des méthodes d'attaque:

Dans ce scénario, nous avons supposé que l'organisation concernée dispose d'une couverture de cyber assurance. Une fois passé le choc initial, en tant que responsable informatique, votre première tâche sera de faire un premier appel téléphonique à votre assureur. Les paragraphes suivants décriront ce à quoi vous pourriez vous attendre au-delà de ce point. Pour commencer, la compagnie d'assurance recommandera d'utiliser deux services distincts:

1) L'urgence technique immédiate est une préoccupation majeure. Une recommandation sera faite pour embaucher une société de conseil en cybersécurité tierce de confiance, avec une ou plusieurs des capacités suivantes, en fonction des besoins spécifiques:

- Experts en récupération de données et de systèmes

- Expérience de négociation de ransomware
- Experts en criminalistique numérique
- Spécialistes de la cybersécurité

La confiance, l'expérience et la compétence prouvée sont les facteurs clés dans ce choix.

2) Pour coordonner la récupération, qui est presque toujours complexe, un coach en récupération de cyberattaque (breach coach) sera engagé. Le coach en récupération de cyberattaque est presque toujours un avocat. Il s'agit de résoudre les problèmes juridiques prévisibles à venir, après une cyberattaque, en fournissant en fait à la fois les conseils de guide expérimenté dans ces circonstances et les conseils juridiques.

L'un des risques les plus courants résultant d'une cyberattaque est que des renseignements personnels identifiables (PII) ou des renseignements personnels sur la santé (PHI) puissent être divulgués. En outre, les données confidentielles de l'entreprise, telles que les brevets ou les informations confidentielles de l'entreprise, peuvent également être menacées. Le rôle du coach en récupération de cyberattaque est de guider l'organisation dans l'identification des exigences liées à la confidentialité des données et de l'aider à retenir les fournisseurs compétitifs, de confiance, pour aider à contrôler et à contenir les dommages post-attaque.

Il s'agit notamment des éléments suivants :

- Embauche de services de surveillance du crédit
- Conseils sur les stratégies de relations publiques (comment communiquer les circonstances de l'incident)
- S'assurer que les obligations post-violation sont respectées pour chacune des juridictions dans lesquelles la société opère.
- Dans de nombreux cas, conseiller sur le choix de service de récupération technique (mentionné au point 1 ci-dessus).

Le fournisseur de cybersécurité, désigné pour effectuer les services immédiats de récupération de données et de systèmes, effectuera une première évaluation du travail à effectuer et fournira un énoncé des travaux à la compagnie d'assurance. Si cela est approuvé, les travaux de récupération se poursuivront, sous la direction du coach en récupération de cyber-attaque.

Les tâches de récupération post-cyberattaque entrent généralement dans l'une des trois catégories suivantes:

1) Négociations de rançon (si l'utilisation d'un rançongiciel est impliquée)

- Collecte de preuves (entre autres, investiguer si le rançonneur a la réputation de prendre l'argent sans livrer de clef de décryptage ou si le rançonneur est sanctionné par les autorités gouvernementales)

The cybersecurity provider appointed to perform the immediate data and system recovery services will perform a first evaluation on the work to be done and provide a Statement of Work (SoW) to the insurance company. If this is approved, the recovery work will go ahead, under the guidance of the breach coach.

Post-cyberattack recovery tasks typically fall in one of three big categories:

1) Ransomware negotiations (if a ransom is involved)

- Evidence collection
- Ransomware negotiation, with the aim of reducing the ransom and still get the decryption key
- Decryption and data recovery

2) Forensics (if data has been extracted)

- Evidence collection
- Root-cause investigation, compromise assessment

3) Post-breach remediation

- Post-breach evidence collection
- Help and remediation for
  - Decrypting data
  - Network vulnerability review
  - Active Directory /Domain Controller
  - Hypervisor infrastructure
  - Email systems vulnerability review
  - Server re-build
  - Backup re-build
- Cloud solution security
- e-Discovery
- Dark web search

The scenario above involves an insurance company, a breach coach and an outsourced technical consulting service. Not all companies are insured, nor will they necessarily have access to all these specific resources. Experience shows however that having access to a team of experts, who deal with these issues every day, make recovery significantly less stressful and increase the chances of a speedier recovery. Another element that invariably helps in such circumstances is a well-structured, well-practiced and well-tested disaster recovery plan. ■

Editors' note: Watch for the second part of this article in the Spring 2023 edition of True North Resilience magazine.

Thibault Dambrine *is an IT consultant with Keyera Corp. (keyera.com) in Calgary, Alberta. At the time of writing, he was working for CyberClan (www.cyberclan.com). The author thanks each and every reviewer that helped make this essay what it has become. Thibault can be reached at dambrine@gmail.com.*

- Négociation de rançon, dans le but de réduire le montant de rançon à payer tout en obtenant la clé de décryptage
- Décryptage et récupération de données

2) Criminalistique (si les données ont été exfiltrées)

- Collecte de preuves
- Enquête sur les causes profondes, évaluation des compromis

3) Correction après la violation

- Collecte de preuves après l'atteinte à la vie privée
- Aide et correction pour
  - Décryptage des données
  - Examen de la vulnérabilité du réseau
  - Active Directory/Contrôleur de domaine
  - Infrastructure de l'hyperviseur
  - Examen de la vulnérabilité des systèmes de messagerie
  - Reconstruction du serveur
  - Reconstruction de sauvegarde
- Sécurité des solutions Infonuagique
- Découverte électronique (eDiscovery)
- Recherche sur le Dark Web

Le scénario que nous venons de décrire implique une compagnie d'assurance, un coach en récupération de cyber-attaque et un service de conseil technique externe. On ne peut pas prendre toutes ces ressources pour acquis. L'expérience montre cependant que le fait d'avoir accès à une équipe d'experts, qui traitent de ces questions tous les jours, rend le processus de récupération beaucoup moins stressant et augmente les chances d'un rétablissement plus rapide. D'autres éléments qui aident invariablement dans de telles circonstances sont un plan de reprise après sinistre (DRP) bien structuré et bien exercé, un plan de continuité des activités (BCP) et une base de données de gestion de la configuration (CMDB) à jour. ■

Note de la rédaction : Surveillez la deuxième partie de cet article dans l'édition du printemps 2023 du magazine de Résiliennce du Vrai Nord.

Thibault Dambrine *est un consultant en TI chez Keyera Corp. (keyera.com) à Calgary, en Alberta. Au moment d'écrire cet article, il travaillait chez CyberClan (www.cyberclan.com). L'auteur remercie tous les critiques qui ont contribué à faire de cet essai ce qu'il est devenu. Thibault est joignable à dambrine@gmail.com.*

CYBERATTACKS: Stakeholder & Responses, Impacts & Trends (Part II)

LA MONTÉE DE LA CYBERCRIMINALITÉ : Quel est le coût réel? (Deuxième Partie)

By/Par Thibault Dambrine

Editors' note: This is the second of two parts. The first part of this article appeared in the Fall 2022 edition of True North Resilience magazine.

Note de la rédaction: Ceci est la deuxième de deux parties. La première partie de cet article a été publiée dans l'édition d'automne 2022 du magazine de Résiliennce du vrai nord.

In this article, I will describe:

- *The impact cyberattacks have on organizations and people*
- *Risk mitigation investments, points of references and trends*

Part 2: The Impact: What is the true cost of Cyberattacks?

Cyberattack recovery is both time-consuming and expensive. In Canada, the average cost of a ransomware attack was USD$1,249,701 in 2021. Source: Emsisoft (see link). There are many aspects and possible damages to consider, understand and remediate. Let's look at a real-life example: the situation of the City of Saint John, the provincial capital of New Brunswick, population 70K. In November 2020, this municipal government organization was victim of a phishing cyberattack. Note the cost of remediation: nearly $3M.

The hack:	The Cost:	
Phishing email – followed by		
• Reconnaissance	• Event Management	$34,421
• Administrative Rights	• Recovery consultant	$902,683
• Lateral Movement	• Forensic Consultants	$295,955
• 13 Nov 2020 Attack	• Third Party Vendors	$460,098
• All Windows Servers Impacted Recovery:	• Equipment	$1,189,141
• Temporary Network Setup	• Overtime	$43,198
• Core Network – 14 Weeks	• Response	$10,681
• Back-Up System – 18 Weeks	• Business Continuity	$14,234
• Impacted Application Recovery (60+)	Estimated Total 6 April 2021	$2,950,409

Source: https://umnb.ca/wp-content/uploads/2021/10/Stephanie-Rackley-Roach-Cybersecurity-SJ-2021-EN.pdf

In this case, we have a public organization with a business email compromise (BEC) situation, no ransomware, the entire cost was spent on recovery services and equipment rebuilding. It can get worse. Over and above ransoms, lack of preparation, poor backup practices and leak of confidential data can add to the cost.

Cyberattacks are pernicious in nature. While the immediate visible impact is significant, there may be more, long-lasting damages. To quantify the full effect cyberattacks, Oxford University researchers have identified at no less than 57 individual adverse effects, split in 5 broad categories. The initial cost of not being able to function as a business is just the beginning. Not all specific effects listed below will be experienced by all organizations. Damage extent however will be in inversely proportion to preparedness.

Dans cet article, nous allons enquêter sur :

- *L'impact des cyberattaques sur les organisations et les individus*
- *Les investissements possibles pour atténuer les risques, ainsi que des points de référence*

Deuxième Partie : L'impact : Quel est le coût réel d'une cyberattaque?

La récupération apres une cyberattaque est à la fois longue et coûteuse. Au Canada, le coût moyen d'une attaque de rançongiciel était de $1,249,701 US en 2021. Source: Emsisoft (voir lien). Il y a de nombreux aspects et dommages possibles à considérer, à comprendre et à corriger. Prenons un exemple concret : la situation de la ville de Saint John, la capitale provinciale du Nouveau-Brunswick, 70 000 habitants. En novembre 2020, cette organisation municipale a été victime d'une cyberattaque d'hameçonnage. Notez le coût de récupération post-cyber-attaque : : près de 3 M$.

Le hack :	Le coût :	
Courriel d'hameçonnage – suivi de		
• Reconnaissance	• Gestion d'événements	34 421 $
• Droits d'administration	• Consultant en récupération	902 683 $
• Mouvement latéral	• Consultation médico-légale	295 955 $
• 13 Nov 2020 Attaque	• Fournisseurs tiers	460 098 $
• Tous les serveurs Windows affectés à la récupération :	• Équipement	1 189 141 $
• Configuration réseau temporaire	• Heures supplémentaires	43 198 $
• Réseau central – 14 semaines	• Réponse	10 681 $
• Système de sauvegarde – 18 semaines	• Continuité d'activité	14 234 $
• Récupération d'applications affectée (60+)	• Total estimé 6 avril 2021	2 950 409 $

Source : https://umnb.ca/wp-content/uploads/2021/10/Stephanie-Rackley-Roach-Cybersecurity-SJ-2021-EN.pdf

Dans ce cas, nous avons une organisation publique avec une situation de compromission des courriels mais pas de rançongiciel. La totalité des coûts totaux a été dépensée sur des services de récupération et de reconstruction. De manière réaliste, cette situation aurait pu être bien pire. Au-delà des problèmes décrits, le manque de préparation, les mauvaises pratiques de sauvegarde et la fuite de données confidentielles auraient pu augmenter le coût..

Les cyberattaques sont de nature pernicieuse. Bien que l'impact visible immédiat soit important, il peut y avoir d'autres dommages durables. Pour quantifier l'effet complet des cyberattaques, des chercheurs de l'Université d'Oxford ont identifié pas moins de 57 effets individuels délétères,

Organizational Cyberharm				
Physical/Digital	**Economic**	**Psychological**	**Reputational**	**Social/Societal**
Damaged or unavailable	Disrupted operations	Confusion	Damaged public perception	Negative changes in public perception (e.g., of technology)
Destroyed	Disrupted sales/turnover	Discomfort	Reduced corporate goodwill	Disruption in daily life activities
Theft	Reduced customers	Frustration	Damaged relationship with customers	Negative impact on nation (e.g., services, economy)
Compromised (e.g., open to access that is unauthorized	Reduced profits	Worry/Anxiety	Damaged relationship with suppliers	Drop in internal organization morale
Infected	Reduced growth	Feeling upset	Reduced business Opportunities	
Exposed/leaked	Reduced investments	Depressed	Inability to recruit desired staff	
Corrupted	Fall in stock price	Embarrassed	Media scrutiny	
Reduced performance	Theft of finances	Shameful	Loss of key staff	
Bodily injury	Loss of finances/capital	Guilty	Loss or suspension of accreditations or certifications	
Pain	Regulatory fines	Loss of self-confidence	Reduced credit scores	
Loss of life	Investigation costs	Low satisfaction		
Prosecution	PR response costs	Negative changes in perception		
Abuse	Compensation payments			
Mistreatment	Extortion payments			
Identity theft	Loss of jobs			
	Scammed			

Source: https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks

Cybersecurity Risk mitigation Investment: How much is enough?

In California, the Security Breach and Information Act was implemented in 2003. This is the earliest cybersecurity-specific law of its type to be implemented. Many states, many countries have followed with their own, Canada's Personal Information Protection and Electronic Documents Act PIPEDA and Europe's General Data Protection Regulation GDPR are examples of those.

Laws are not designed to dictate the use of specific technologies, but rather provide measures for "data protection requirements".

When evaluating what the "right amount" of investment in cybersecurity may be, understanding how well those measures are met is one of the ways to gauge what may be required.

There are three points to examine, with the aim to achieve a "reasonable" or "adequate" security balance:

1) The basic need to meet the internal security goals, corporate data protection and business continuity
2) The need to meet external legal obligations imposed by privacy laws, such as PIPEDA or GDPR.
3) The need to balance costs of security and insurance requirements, against the value of the data and the effort required to access that same data.

When considering cyberattack risk mitigation, organizations have the following options:

- Accept the risk > not a desirable position
- Avoid the risk > not a realistic position

Cyberharm organisationnel				
Physique/Numérique	**Économique**	**Psychologique**	**Réputation**	**Social/Sociétal**
Endommagé ou indisponible	Opérations perturbées	Confusion	Perception du public endommagée	Changements négatifs dans la perception du public (p. ex., de la technologie)
Détruit	Ventes/chiffre d'affaires perturbés	Gêne	Réduction du goodwill de l'entreprise	Perturbation des activités de la vie quotidienne
Vol	Réduction du nombre de clients	Frustration	Relation endommagée avec les clients	Impact négatif sur la nation (p. ex., services, économie)
Compromis (p. ex., ouvert à l'accès non autorisé	Réduction des bénéfices	Inquiétude/anxiété	Relation endommagée avec les fournisseurs	Baisse du moral interne de l'organisation
Infecté	Croissance réduite	Se sentir contrarié	Réduction des opportunités d'affaires	
Exposé/fuite	Réduction des investissements	Déprimé	Incapacité à recruter le personnel souhaité	
Corrompu	Chute du cours de l'action	Embarrassé	Examen minutieux des médias	
Performances réduites	Vol de finances	Honteux	Perte de personnel clé	
Blessures corporelles	Perte de finances/capital	Coupable	Perte ou suspension d'accréditations ou de certifications	
Douleur	Amendes réglementaires	Perte de confiance en soi	Réduction des cotes de crédit	
Perte de vie	Coûts de l'enquête	Faible satisfaction		
Poursuite	Coûts d'intervention des RP	Changements négatifs dans la perception		
Abus	Indemnités			
Mauvais traitements	Paiements par extorsion			
Vol d'identité	Perte d'emplois			
	Arnaquer			

Source : https://www.ox.ac.uk/news/2018-10-29-researchers-identify-negative-impacts-cyber-attacks

divisés en 5 grandes catégories. Le coût initial de ne pas pouvoir fonctionner en tant qu'entreprise n'est que le début. Toutes les organisations ne subiront pas tous les effets spécifiques énumérés ci-dessus. Toutefois, l'étendue des dommages sera inversement proportionnelle à la préparation contre ce genre d'attaque.

Investissement dans l'atténuation des risques de cybersécurité : combien suffit-il?

En Californie, le Security Breach and Information Act a été votée en 2003. Il s'agissait alors d'une première dans ce domaine. De nombreux États et de nombreux pays ont emboîté le pas, mettant en œuvre leur propre lois sur la protection des renseignements personnels et les documents électroniques.

Au Canada, PIPEDA et le Règlement général sur la protection des données de l'Europe, le GDPR en sont des exemples.

Ces lois ne sont pas conçues pour dicter l'utilisation de technologies spécifiques, mais plutôt pour fournir des mesures pour les « exigences de protection des données ». Lors de l'évaluation de ce que peut être le « montant approprié » d'investissement dans la cybersécurité, comprendre si ces mesures sont respectées est l'un des moyens d'évaluer ce qui peut être nécessaire.

Il y a trois points à examiner, dans le but d'atteindre un équilibre de sécurité « raisonnable » ou « adéquat » :

1) Le besoin fondamental d'atteindre les objectifs de sécurité interne, la protection des données de l'entreprise et la continuité des activités
2) La nécessité de respecter les obligations légales externes imposées par les lois sur la protection de la vie privée, telles que PIPEDA ou le GDPR.
3) La nécessité d'équilibrer les coûts des exigences de sécurité et d'assurance, par rapport à la valeur des données et l'effort requis pour accéder à ces mêmes données.

Lorsqu'elles envisagent d'atténuer le risque de cyberattaque, les organisations disposent des options suivantes:

- Accepter le risque > Une position peu souhaitable
- Éviter le risque > Une position peu réaliste

- Transfer the risk >
  Get cybersecurity insurance coverage and hope that they will absorb the cost if the risk is realized.
- Reduce the risk > get outside cybersecurity help from a specialized outsource company to harden the IT infrastructure.
- Hedge against the risk > Reduce and transfer the risk, by implementing both (4) and (5) - the "belt and suspenders" approach.

The following graphs show a clear correlation between the global increased cost of cyberattacks and cyber insurance premiums. For many organizations, transferring the risk with cybersecurity insurance coverage may soon be conditional to showing that every effort has been made to harden against cyber-attacks.

An investment in reducing cyber risk has both short and long-term benefits:

- **In the short-term:**
  - The cost of prevention is invariably cheaper than the cost of recovering from a cyberattack.
  - Being prepared is being ready. Industry standard cybersecurity measures are likely to become a pre-requisite to being able to get cyber insurance coverage.
- **In the long-term:**
  - Reducing the chance of an attack being successful.
  - Pro-actively protecting data improves the safety of information related to individuals such as personnel, clients, Personally Identifiable Information (PII), Protected Health Information (PHI) data and any other sensitive information.
  - Customers have greater confidence in a supplier who invests in data security.
  - Some cybersecurity providers offer warranties, in the event of a network breach, for customers covered under their managed monitoring services.

The aim is to ensure the data in custody would be reasonably safe from attacks, while remaining functional and usable. There must be a balance. Over-securing could either make the data unusable or simply cost more than the value being protected.

Conclusions

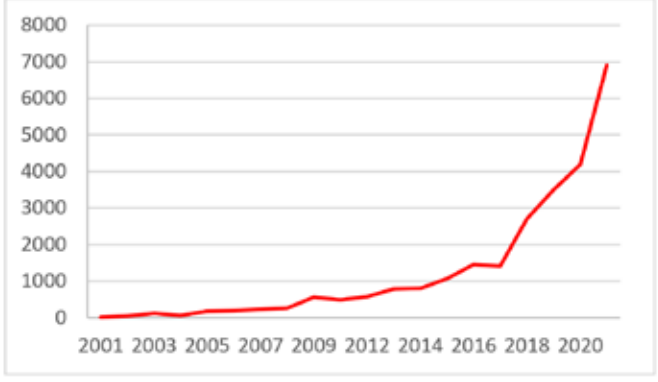
In 1736, Benjamin Franklin helped create the "Union Fire Company" in Philadelphia. This became a model for subsequent modern municipal fire departments. On the topic of urban fire damage potential, he was famously quoted for advising that "An ounce of prevention is worth a pound of cure."

Using the fire analogy, arson attack methods have not changed much for centuries. By comparison, cyberattacks constantly morph and evolve. They are moving targets. Defending against those is a continuous challenge to anticipate and adapt. Successful or not, instances of cyberattacks are increasingly common. In the past, companies who fell victim to those attacks experienced some measure of "shame" for having to admit that they had been hacked. The new reality is that for most organizations, the current outlook on cyberattacks is closer to "will we be prepared, when it happens?"

Cyberattacks may never totally be eradicated. The key question is: What can a company or organization do, when planning for cybersecurity protection? Security in layers, including but not limited to the following elements is a good start:

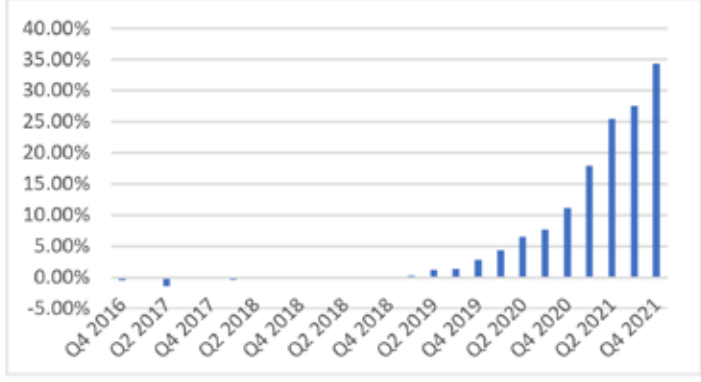
- Top-level sponsorship for cybersecurity initiative is number one
  - People – setting up security training, phishing simulations, tabletop exercises to walk through security exposure scenarios
  - Processes – implementing a disaster recovery plan, complete with yearly disaster recovery practices, reviews and updates

Amount of monetary damage caused by reported cybercrime to the FBI Internet Crime Complaint Center (IC3) from 2001 to 2020 (in million U.S. dollars)



Source: https://www.ic3.gov/Home/AnnualReports
Note: 2010 figure not available from IC3

Premium Change for Cyber Insurance Coverage, Q4 2016 - Q4 2021



Sources: https://www.ciab.com/download/31507/, https://digitallatestnews.in/cyber-premiums-quickly-grew-74-in-2021-fitch/

- Transférer le risque > Obtenir une couverture d'assurance cybersécurité en espérant qu'ils absorberont le coût si le risque est réduit.
- Réduire les risques > Obtenir l'aide extérieure en matière de cybersécurité d'une société externe, spécialisée dans la sécurité informatique.
- Se couvrir contre le risque > Réduire et transférer le risque, en mettant en œuvre à la fois (3) et (4) - l'approche « ceinture et bretelles ».

Les graphiques ci-dessous montrent une corrélation claire entre l'augmentation mondiale du coût des cyberattaques et les primes de cyber assurance. Pour de nombreuses organisations, le transfert du risque avec une couverture d'assurance cybersécurité pourrait bientôt être conditionnel à montrer que tous les efforts ont été faits pour se préparer contre les cyberattaques.

Un investissement dans la prévention contre les cyber risques présente des avantages à court et à long terme :

- **À court terme :**
  - Le coût de la prévention est invariablement moins cher que le coût de la récupération d'une cyberattaque.
  - Être préparé, c'est être prêt. Les mesures de cybersécurité de base sont maintenant une condition préalable à l'admissibilité pour une couverture de cyber assurance.
- **À long terme :**
  - Réduire les chances de succès d'une attaque.
  - La protection proactive des données améliore la sécurité des informations relatives aux individus tels que le personnel, les clients, les informations personnellement identifiables (PII), les données d'information sur la santé protégée (PHI) et toute autre information sensible.
  - Les clients ont davantage confiance en un fournisseur qui investit dans la sécurité des données.
  - Certains fournisseurs de cybersécurité offrent des garanties en cas de violation du réseau, pour les clients couverts par leurs services de surveillance gérés.

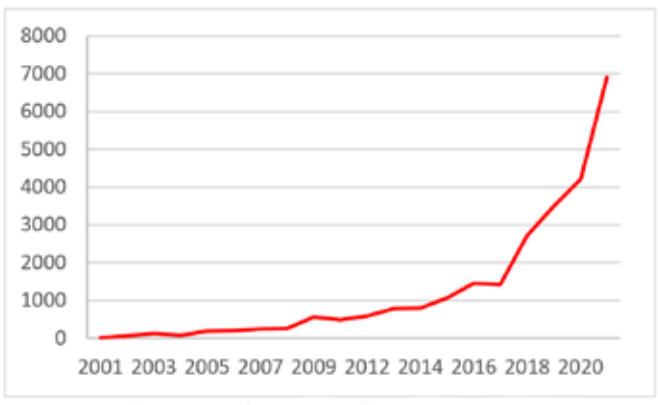
L'objectif est de s'assurer que les données conservées soient à l'abri des attaques, tout en restant fonctionnelles et utilisables. Il doit y avoir un équilibre. Une sécurisation excessive pourrait soit rendre les données inutilisables, ou simplement coûter plus cher que la valeur protégée.

Conclusion

En 1736, Benjamin Franklin était l'un des fondateurs de la « Union Fire Company » à Philadelphie. Cette organisation est devenue un modèle pour les services pompier municipaux modernes. Au sujet du potentiel de dommages causés par les incendies urbains, son commentaire célèbre et souvent cité : « une once de prévention vaut une livre de guérison. »

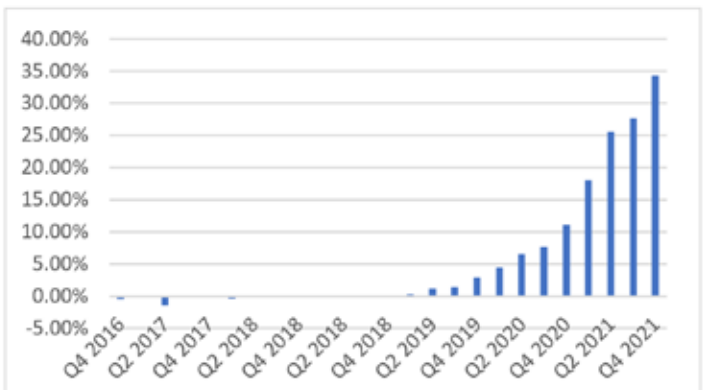
En utilisant l'analogie du feu, les méthodes de démarrage d'incendie criminel n'ont pas beaucoup changé depuis des siècles. En comparaison, les cyberattaques se transforment et évoluent constamment. Ce sont des cibles mouvantes. Se défendre contre ces attaques est un défi continu, obligeant chaque entité connectée à Internet à anticiper et à s'adapter en permanence. Réussies ou non, les cas de cyberattaques sont de plus en plus fréquents. Dans le passé, les entreprises victimes de telles attaques ont éprouvé une certaine « honte » d'avoir dû admettre qu'elles avaient été

Montant des dommages pécuniaires causés par la cybercriminalité signalée au FBI Internet Crime Complaint Center (IC3) de 2001 à 2020 (en millions de dollars américains)



Source : https://www.ic3.gov/Home/AnnualReports
Note : Chiffre de 2010 non disponible à partir d'IC3

Augmentation des primes pour la couverture d'assurance cyber T4 2016 - T4 2021



Sources : https://www.ciab.com/download/31507/, https://digitallatestnews.in/cyber-premiums-quickly-grew-74-in-2021-fitch/

- Technologies – firewalls, EDR, SIEM, UEBA, Email protection, network segmentation, zero-trust security structures, Multi-Factor Authentication (MFA) and automated monitoring to start with
- Recurring security audits, penetration test exercises, network, and infrastructure reviews, using outside, independent specialized vendors

In a not-so-distant future, a consistent focus on prevention – minimum cybersecurity protection – as opposed to remediation, will likely become default practice. If not fewer attacks, this should lead to fewer successful attacks.

One could be tempted to read the article above as an elaborate promotion for cybersecurity, legal and insurance services. The reality is that it aims to educate. In. doing so, it illustrates that Mr. Franklin's 1736 observations still stand today: preventing is less expensive than curing. Ω

References & Abbreviations:

- **BEC** – Business Email Compromise - scam targeting companies which have foreign suppliers and use wire transfer. BEC relies heavily on social engineering.
- **Cryptojacking** – the act of hijacking a computer to mine cryptocurrencies against the users will, through websites, typically while the user is unaware. Cryptocurrencies mined the most often are privacy coins, with hidden transaction histories—such as Monero and Zcash.
- **eDiscovery** – discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests, where the information sought is in electronic format.
- **EDR** – Endpoint Detection and Response - a cybersecurity technology that continually monitors an "endpoint" (e.g. mobile phone, laptop, Internet-of-Things device) to mitigate malicious cyber threats.
- **GDPR** – General Data Protection Regulation – the European Union EU law on data protection and privacy
- **MFA** – Multi-Factor Authentication
- **PHI** – Protected Health Information, interpreted rather broadly and includes any part of a patient's medical record or payment history.
- **PII** – Personally Identifiable Information, is any information related to an identifiable person.
- **PIPEDA** – Personal Information Protection and Electronic Documents Act – the Canadian law relating to data privacy.
- **RaaS** – Ransomware as a Service is a business model used by tech-savvy criminals selling or renting working ransomware technology to other cybercriminals.
- **SIEM** – Security information and Event Management systems provide real-time analysis of security alerts generated by several combined sources, including applications and network services.
- **Social Engineering** – the psychological manipulation of people into performing actions or divulging confidential information.
- **UEBA** – User and Entity Behavior – is software which using AI, learns normal user conduct patterns. It subsequently can trigger alarms if deviations from "normal" behavior in real-time.
- **VNC** – **Virtual Network Computing** – is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. Ω

piratées. La nouvelle réalité est que, pour la plupart des organisations, la perspective actuelle sur les cyberattaques est plus proche de « serons-nous préparés, quand cela se produira? ».

Les cyberattaques ne seront peut-être jamais totalement éradiquées. À ce sujet, la question clé à garder en tête est la suivante: comment une entreprise ou une organisation devrait-elle planifier sa protection contre des cyberattaques? La sécurité à aspects multiples. La liste d'éléments qui suit est un bon début de considérations possibles :

- Un parrainage (sponsorship) de haut niveau pour l'initiative de cybersécurité est le numéro un. Une personne de l'exécutif de la compagnie doit être le chef de l'initiative.
  - Aspect humain : la mise en place d'une formation à la sécurité, de simulations d'hameçonnage, d'exercices sur table pour parcourir les scénarios d'exposition à la sécurité
  - Aspect des processus : la mise en œuvre d'un plan de reprise après sinistre. Ce plan doit etre pratiqué et revu au mmoins une fois par an
  - Aspect des technologies : la mise en place de murs coupe-feu (firewall), technologie et réponse des terminaux (EDR), gestion des informations et des événements de sécurité (SIEM), analyse du comportement des utilisateurs et des entités (UEBA), protection des courriels, segmentation du réseau, structures de sécurité zéro-cofinance, authentification multi facteur (MFA) et surveillance automatisée
  - Mise en place d'audits de sécurité récurrents, exercices de tests d'intrusion, examens du réseau et de l'infrastructure, faisant appel à des fournisseurs spécialisés, externes et indépendants

En ce qui concerne l'approche a la cybersécurité, dans un avenir proche, on peut s'attendre à ce que la prévention devienne presque un réflexe. Si cette approche ne peut pas garantir qu'il n'y ait moins d'attaques, cela devrait au moins conduire à moins d'attaques réussies.

On pourrait être tenté de lire l'article ci-dessus comme une promotion élaborée pour les services de cybersécurité, juridiques et d'assurance. La réalité est qu'il vise à éduquer. Ce faisant, il illustre que les observations de M. Franklin de 1736 sont encore valables aujourd'hui : prévenir coûte moins cher que guérir. Ω

ABOUT THE AUTHOR

Thibault Dambrine *is an IT consultant with Keyera Corp. (keyera.com) in Calgary, Alberta. At the time of writing, he was working for CyberClan (www.cyberclan.com). The author thanks each and every reviewer that helped make this essay what it has become. Thibault can be reached at dambrine@gmail.com.*

Références & Abréviations:

- **BCP** – Plan de continuité des activités – un plan décrivant un système de procédures de prévention et de récupération, en cas de menaces opérationnelles pour une entreprise. Le plan garantit que le personnel et les biens sont protégés et sont en mesure de fonctionner rapidement en cas de sinistre.
- **BEC** – Business Email Compromise – une arnaque ciblant les entreprises qui ont des fournisseurs étrangers et utilisent le virement bancaire. BEC s'appuie fortement sur l'ingénierie sociale.
- **CMDB** – Configuration Management Database – terme ITIL désignant une base de données utilisée par une organisation pour stocker des informations sur les actifs matériels et logiciels.
- **Cryptojacking** - l'acte de détourner un ordinateur pour extraire des cryptomonnaies contre les utilisateurs le fera, via des sites Web, généralement alors que l'utilisateur n'est pas au courant. Les cryptomonnaies extraites le plus souvent sont des pièces privées, avec des historiques de transactions cachés—tels que Monero et Zcash.
- **DRP** – Disaster Recovery Plan – une approche documentée et structurée qui décrit comment une organisation peut rapidement reprendre le travail après un incident imprévu. Un PRD est un élément essentiel d'un plan de continuité des activités (PCA).
- **eDiscovery** – la découverte, dans des procédures judiciaires telles que des litiges, des enquêtes gouvernementales ou des demandes en vertu de la Freedom of Information Act, lorsque les informations recherchées sont en format électronique.
- **EDR** – Endpoint Detection and Response – une technologie de cybersécurité qui surveille en permanence un « point de terminaison » (p. ex. téléphone mobile, ordinateur portable, appareil Internet des objets) pour atténuer les cybermenaces malveillantes.
- **RGPD** – Règlement général sur la protection des données – la législation de l'Union européenne sur la protection des données et de la vie privée
- **ITIL** – Information Technology Infrastructure Library – un ensemble de pratiques détaillées pour les activités informatiques telles que la gestion des services informatiques (ITSM) et la gestion des actifs informatiques (ITAM) qui se concentrent sur l'alignement des services informatiques sur les besoins de l'entreprise.
- **MFA** – Authentification multifacteur
- **PHI** – Protected Health Information – interprété de manière assez large et inclut toute partie du dossier médical ou de l'historique de paiement d'un patient.
- **PII** – Informations personnellement identifiables – toute information liée à une personne identifiable.
- **LPRPDE** – Loi sur la protection des renseignements personnels et les documents électroniques – la loi canadienne relative à la confidentialité des données.
- **RaaS** – Ransomware as a Service – un modèle commercial utilisé par les criminels férus de technologie qui vendent ou louent une technologie de ransomware fonctionnelle à d'autres cybercriminels.
- **SIEM** – Security information and Event Management systems – un système logiciel spécialisé fournissant une analyse en temps réel des alertes de sécurité générées par plusieurs sources combinées, y compris les applications et les services réseau.
- **Ingénierie sociale** – la manipulation psychologique des personnes pour qu'elles effectuent des tâches ou divulguent des informations confidentielles.
- **UEBA** – User and Entity Behavior – est un logiciel qui, à l'aide de l'IA, apprend les modèles de conduite normaux des utilisateurs. Il peut ensuite déclencher des alarmes en cas d'écart par rapport au comportement « normal » en temps réel.
- **VNC** – Virtual Network Computting – un système graphique de partage de bureau qui utilise le protocole RFB (Remote Frame Buffer) pour contrôler à distance un autre ordinateur. Ω

À PROPOS DE L'AUTEUR
Thibault Dambrine *est un consultant en TI chez Keyera Corp. (keyera.com) à Calgary, en Alberta. Au moment d'écrire cet article, il travaillait chez CyberClan (www.cyberclan.com). L'auteur remercie tous les critiques qui ont contribué à faire de cet essai ce qu'il est devenu. Thibault est joignable à dambrine@gmail.com.*