Cyberattacks: Stakeholder & Responses, Impacts & Trends

Thibault Dambrine - May 2022

Introduction

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%.

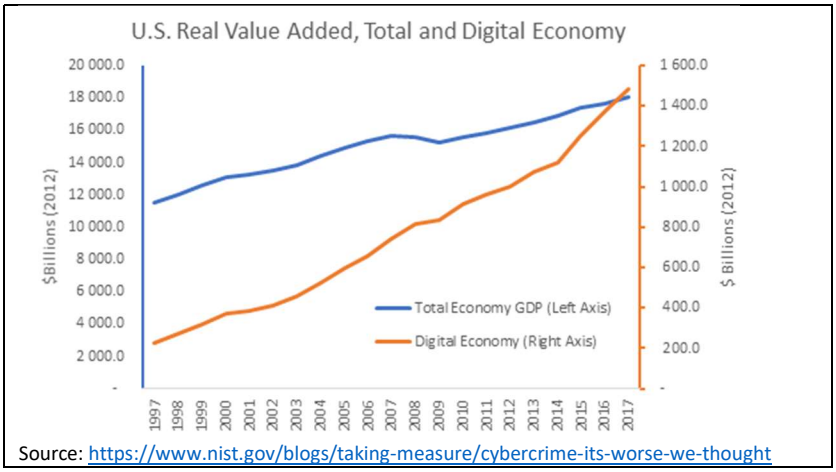
Today, cybercrimes openly reported in the news are no longer unusual events. What has changed however is that such attacks tend to affect larger number of individuals, stranding airline passengers, causing gasoline shortages, leaking banking customer data, crippling hospitals and more. The damage is real, it is visible, it is far-reaching and it affects people's lives. This is not a "victimless crime".

In this article, I will describe:

- Cyberattack response stakeholder roles and processes
- The impact cyberattacks have on organizations and people
- Risk mitigation investments, points of references and trends

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:

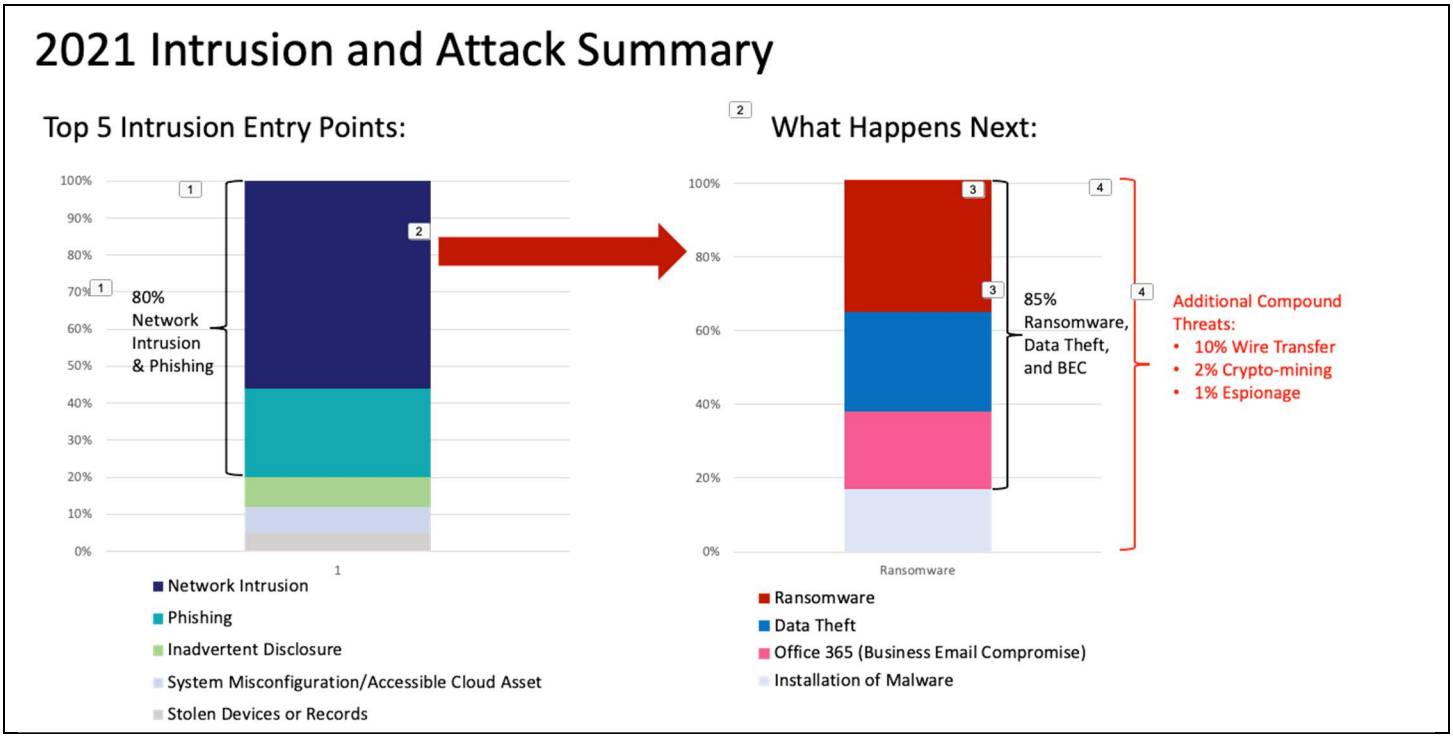
- Data, in digital form, has become so integral to most company functions that it is now considered an asset.
  - Companies, organizations, protect their assets against risk with insurance policies. Buildings and vehicles come to mind. Data, either in motion (think of e-commerce, process control systems)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

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.

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	➢ Equipment	$1,189,141
Recovery:	➢ Overtime	$43,198
➢ Temporary Network Setup	➢ Response	$10,681
➢ Core Network – 14 Weeks	➢ Business Continuity	$14,234
➢ Back-Up System – 18 Weeks	Estimated Total 6 April 2021	$2,950,409
➢ Impacted Application Recovery (60+)		

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.

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

Part 3: 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

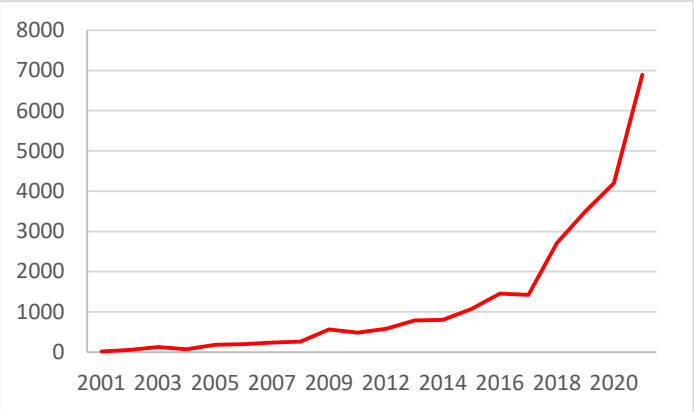
2) The need to meet external legal obligations imposed by privacy laws, such as PIPEDA or GDPR.
3) The need to balance costs of security and insurance requirements, against the value of the data and the effort required to access that same data.

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

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

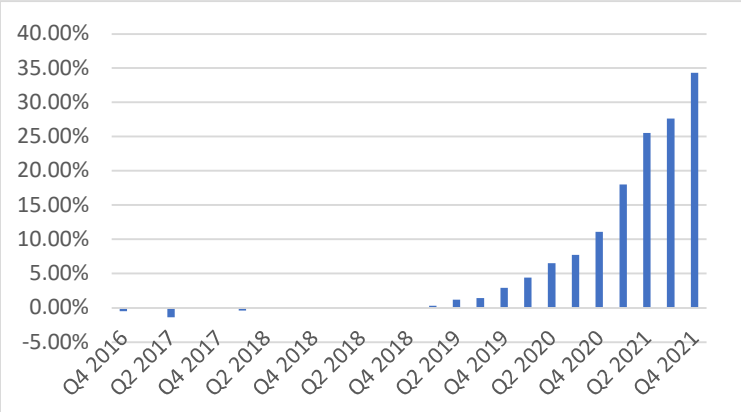
The graphs below show a clear correlation between the global increased cost of cyberattacks and cyber insurance premiums. For many organizations, transferring the risk with cybersecurity insurance coverage may soon be conditional to showing that every effort has been made to harden against cyber-attacks.

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/

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
  - 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.

References & Abbreviations:

- BCP – Business continuity plan – a plan describing a system of prevention and recovery procedures, in case of operational threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster.
- BEC – Business Email Compromise – a scam targeting companies which have foreign suppliers and use wire transfers. BEC relies heavily on social engineering.
- CMDB – Configuration Management Database – an ITIL term for a database used by an organization to store information about hardware and software assets.
- Cryptojacking – the act of hijacking a computer to mine cryptocurrencies against the user's 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.
- DRP – Disaster Recovery Plan – a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident. A DRP is an essential part of a business continuity plan (BCP).
- eDiscovery – the 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
- ITIL – Information Technology Infrastructure Library – a set of detailed practices for IT activities such as IT service management (ITSM) and IT asset management (ITAM) that focus on aligning IT services with the needs of the business.
- 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 – 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 – a business model used by tech-savvy criminals selling or renting working ransomware technology to other cybercriminals.
- SIEM – Security Information and Event Management systems – a specialized software system providing 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 Analytics – is software which uses AI, and learns normal user conduct patterns. It subsequently can trigger alarms if deviations from "normal" behavior in real-time.
- VNC – Virtual Network Computing – a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer.

Thibault Dambrine is a pre-sales consultant with www.cyberclan.com. The author thanks each and every reviewer that helped make this essay what it has become. He can be reached at thibault.dambrine@cyberclan.com or at dambrine@gmail.com