NEGATIVE PID

WHITE PAPER

CYBERCRIME VICTIM SUPPORT

BUILDING A CASE FOR IDENTITY THEFT VICTIM SUPPORT IN THE WORKPLACE

January 2024

https://negativepid.com

NEGATIVE PID

Contents

I. Introduction

CYBERCRIME IN NUMBERS

Source: aag-it.com

1 Billion
Emails exposed in a year, affecting 1 in 5 Internet users

4.35 Million
USD is the average cost of a data breach for a company in 2022

236 Million
Ransom attacks occurred globally in the first half of 2022

1 in 2
American Internet users had their account breached in 2021

53.3 Million
US citizens were affected by cybercrime in the first half of 2022

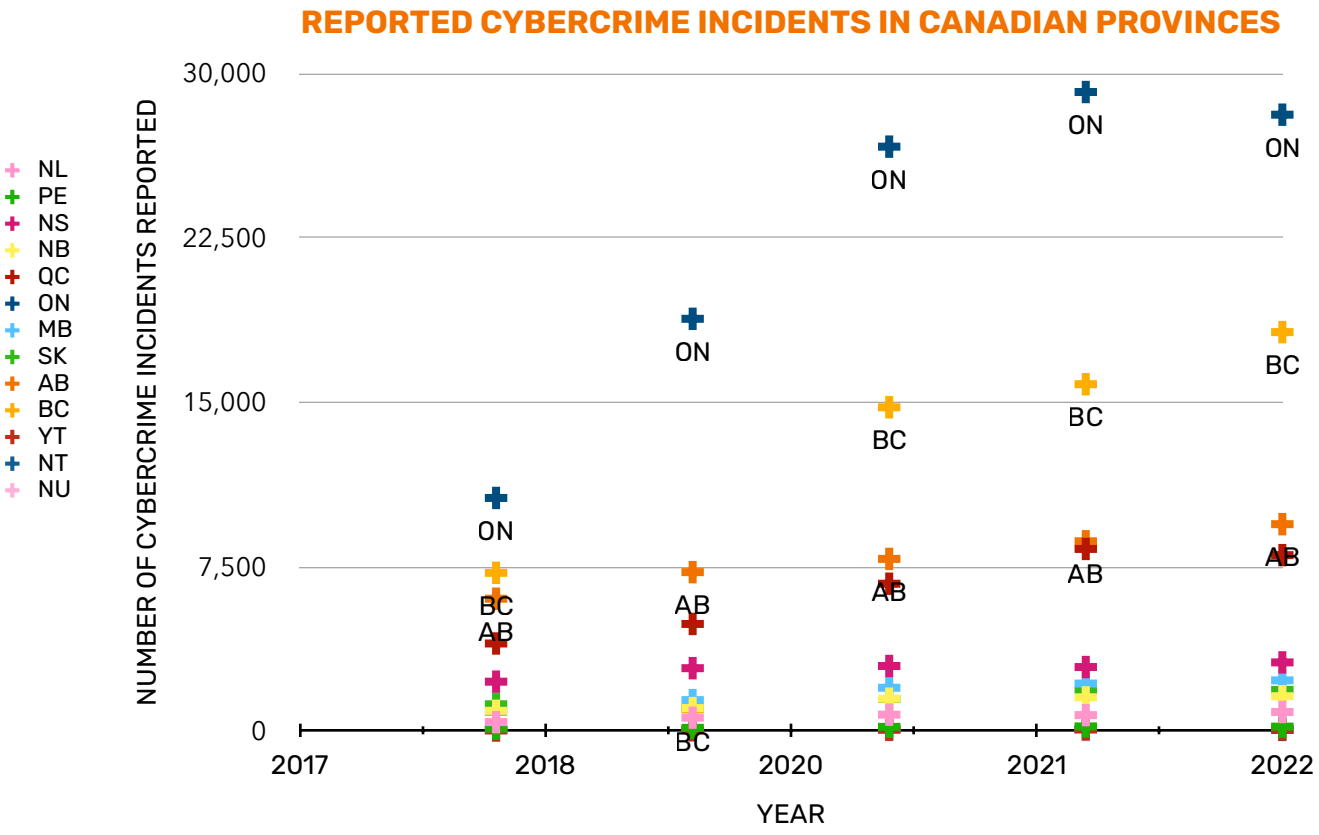
1 in 10
US organizations have no insurance against cyber attacks

358%
Increase in cybercrime in 2020 compared to 2019

Phishing
The most common cyberthreat for businesses and individuals

Cybercrime is on the rise globally, affecting businesses as well as individuals. Indeed, for every business impacted, there are thousands of individuals who suffer the consequences of stolen identity and confidential information. These individuals can be employees of the company that has been breached or employees of their customers and business partners.

According to the Canadian Identity Theft Support Centre, in 2008 the cost of identity theft in Canada only was **$7.2 billion dollars** and affected approximately **2.25 million people** (representing **9.1 per cent** of the population).



Source: Statistics Canada

In most cases, as breached companies tend not to advertise such incidents, victims of identity theft are not even aware that they have become victims until it's too late. And while identity theft has become a common crime, its

consequences are serious. Identity theft victims suffer both from financial losses and psychological distress.

A stolen identity can:

- Ruin one's credit score
- Disrupt ordinary banking activities
- Reveal sensitive medical information
- Be used by criminal organizations to commit other crimes
- Result in problems with the law
- Ruin one's personal and professional reputation

Ultimately, identity theft can threaten the livelihood of the victim and their families. Clearing one's reputation after such events can take several months, if not years, deteriorating the victim's mental health and productivity at work.

In most cases, HR and management are not equipped to deal with such issues, leaving the employee unsupported or even penalized for a situation that they have no control over.

And while the remediation of technical aspects is straightforward, human factors affect both **operational impact** and **reputational damage**, leaving the company to deal with open ended issues and uncertainty.

The purpose of this white paper is to educate on the impact of cybercrime on its victims - companies and individuals - and demonstrate how implementing a cybercrime victim support policy is advantageous both for the victim and for their employer.

We will provide useful insights to **calculate the ROI** of such policies, and give you the tools to present a strong case to upper management for their adoption.

II. The impact of identity theft on victims

When one's identity is stolen, consequences can have significant and far-reaching effects on its victims, both financially and emotionally.

Some common consequences are:

- **Financial Losses**: Identity theft often results in immediate financial losses for the victim. Fraudulent transactions, unauthorized withdrawals, or credit card charges can quickly accumulate, leading to substantial monetary damages.

- **Credit Damage**: When an identity thief misuses personal information to open new credit accounts or default on existing ones, it can severely damage the victim's credit score. Repairing this damage can be time-consuming and challenging.

- **Emotional Distress**: Victims often experience high levels of stress, anxiety, and feelings of violation. The invasion of privacy and the loss of control over personal information can lead to emotional turmoil.

- **Legal Complications**: Resolving identity theft can involve complex legal procedures. Victims may need to work with law enforcement, credit bureaus, and financial institutions to prove their innocence and rectify fraudulent activities.

- **Strain on Relationships**: Dealing with the aftermath of identity theft can strain personal relationships. The stress and financial strain can affect family dynamics and relationships with friends or employers.

- **Reputational Damage**: In cases where the thief commits crimes or engages in unethical behaviour using the victim's identity, the victim's reputation may be tarnished, impacting their personal and professional life.

- **Time and Effort for Resolution**: Rectifying the damage caused by identity theft is time-consuming. Victims often spend significant amounts of time gathering evidence, working with authorities, and communicating with various institutions to restore their identity.

- **Long-Term Impact:** Even after the immediate issues are resolved, the impact of identity theft can linger. Ongoing monitoring of credit reports and financial accounts becomes necessary, creating a lasting sense of insecurity and vigilance.

III. The impact of identity theft on organizations

Statistics from the US Center for Prevention and Health Services show that untreated mental health concerns result in substantial costs for businesses—**$60,000 annually** for one organization and **$105 billion nationwide**.

Employees not dealing with mental health conditions can also significantly impact business costs. According to Gallup, low morale costs American

businesses up to **$550 billion a year** due to lost productivity, including absenteeism, illness, requests of extended leaves of absence, and other problems.

OPERATIONAL IMPACT

- Employees with unresolved depression experience a **35% reduction in productivity**.
- Depression causes an average of **31.4 missed days per year** for an individual. The cost of a missed workday is estimated to be **$340 per day** for full-time employees and **$170 per day** for part-time employees.
- Mentally distressed workers have a **3.5 times higher** likelihood of suffering from **substance use** disorders which contributes to more missed work.
- **Presenteism** (coming to work when one is ill, injured, or otherwise unable to function at full capacity on the job) is a by-product of mental distress. This adds up to another **27.9 days lost** annually due to reduced productivity.

When an employee leaves their position, voluntarily or not, companies face additional costs and loss of productivity due to additional workloads on remaining employees, recruitment costs, training new employees, and loss of institutional knowledge.

The cost of mental health treatment is a fraction of these costs, and yet many people do not seek treatment because they cannot afford it or are afraid of the stigma attached to mental illness.

REPUTATIONAL DAMAGE

A Forbes Insight report found that **46%** of organizations had suffered reputational damage as a result of a data breach and **19%** of organizations suffered reputation and brand damage as a result of a third-party security breach.

NEGATIVE PID

According to the IBM & Ponemon Cost of a Data Breach Report 2020, **80%** of breached organizations state that customer personally identifiable information (PII) was compromised during the breach.

While the average **cost per lost or stolen record was $146** across all data breaches, those containing customer PII cost businesses **$150 per record**—as well as the threat of customers losing faith in the company and turning elsewhere.

Deloitte determined that up to **90%** of the total costs in a cyberattack occur beneath the surface. Hidden costs, like damaged credibility, can affect a business for years after a breach.

This is why, as Fundera reports, **60%** of small businesses that are victims of a cyberattack **go out of business within six months**.

IV. A proactive approach to mitigate cybercrime victim costs

The occurrence of data breaches is an unfortunate reality. Beyond the technical ramifications, the human toll of these incidents cannot be understated. It is no longer possible to ignore the need for supporting individuals who have been victims of cybercrime, and in particular those whose PIIs have been exposed.

Recognizing the human impact is crucial for organizations seeking to cultivate a resilient workforce and supply chain.

To address the emotional aftermath of a data breach, organizations can implement counselling services as part of their cybersecurity response plan.

This proactive approach helps individuals cope with the psychological impact, facilitating a faster and more effective recovery.

Employees who feel that their employer cares about their overall well-being are:

- **69%** less likely to actively search for a new job
- **3x** more likely to be engaged at work
- **71%** less likely to report experiencing burnout
- **36%** more likely to be thriving in their overall lives
- **5x** more likely to strongly advocate for their company as a place to work

At the same time, offering counselling services to a partner's or customer's workforce whose credentials have been stolen due to a data breach can show accountability for the incident. This will go a long way in retaining their trust and reduce legal costs on compensation for damages in a court of law.

Indeed, according to US law, victims of a data breach can sue for:

- The recovery for unauthorized charges to their accounts
- Damage to their credit
- Cost of credit repair or monitoring
- Time and expense associated with investigating and resolving identity theft and **emotional distress**.

Many courts have held that data breach victims are able to bring a claim even if they have not yet noticed any signs of identity fraud. This is based on the understanding that those who had their information stolen face an increased risk of identity theft far into the future.

Adopting a contingency plan that includes identity theft victim support can help you control the costs and improve the perception of your brand.

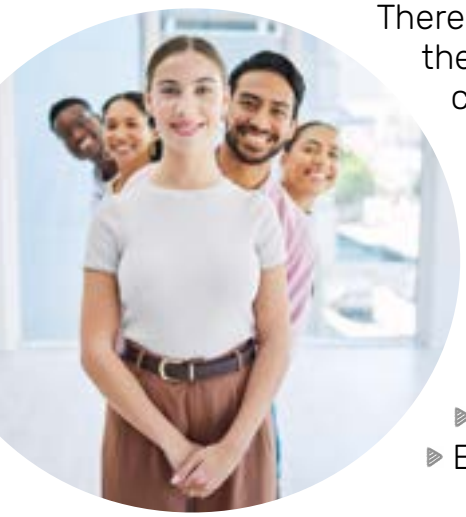
Ultimately, victims will less likely sue for compensation and damages when they feel that whomever is responsible for the data leakage is making an effort to support them.

NEGATIVE PID

V. Business cases for cybercrime victim support

With the increasing prevalence of cybercrime, individuals are not only facing financial losses but also psychological distress. Victims often experience anxiety, stress, and a sense of violation, which can have long-lasting effects on their well-being and their productivity at work.

USE CASES FOR IDENTITY THEFT VICTIM SUPPORT



There is a growing need for specialized support services tailored to the unique challenges faced by cybercrime victims. Existing counselling services may not fully address the specific issues related to digital crimes, creating a gap in the market.

Such services can cater to individuals who have fallen victim to cybercrimes such as online fraud, identity theft, cyberbullying, or any form of digital harassment.

These can be:

- Employees of the company that has been breached
- Employees of partner companies or customers

Furthermore, cybercrime victim support counselling can also be beneficial to management and HR personnel who deal with such employees and need guidance on how to support them.

SUCCESS CRITERIA

Any successful cybercrime victim support service should include the following key features:

- **Specialized Expertise**: The counsellors need to be trained to understand the nuances of cybercrimes and their impact on mental health and its dynamics in the workplace.
- **Confidentiality and Security**: Recognizing the sensitive nature of cyber incidents, the counselling sessions should always prioritize client privacy and data security.

- **A flexible support model**: You need to be prepared to one-time counselling sessions for those in need of immediate assistance and continuous support for long-lasting consequences on the individual.

- **Partnerships**: Partnerships with cybersecurity insurance providers or group insurances will give you the option to bundle the services and obtain advantageous deals.

Collaboration with cybersecurity firms to **promote the service** as an essential component of a comprehensive security plan. At the same time, educational campaigns should be conducted amongst employees to **raise awareness** about the psychological impact of cybercrimes and the availability of support services.

MEASURING THE IMPACT

To measure the impact of a cybercrime victim support initiative, there are three main metrics to take into account:

- **The number of subscribers**: You can estimate the number of subscribers to the program with the help of current available statistics on cybercrime

victims and your HR data: both in Canada and in the US, **9%** of the population is affected by identity theft. You can apply the same percentage to your workforce and apply a correction based on your own records of absenteeism, presenteism, extended leaves, etc.

- **Customer satisfaction ratings**: You can measure the satisfaction of the employees participating in the program with random surveys. This, however, should be performed by a third party, as you do want to keep the participation confidential.

- **Effectiveness in reducing psychological distress**: You will need to put in place a system to measure the trend of your HR records before the start of the program and throughout the program to compare performance.

VI. How to calculate the ROI for a cybersecurity victim support initiative

Calculating the Return on Investment (ROI) for a counselling service for cybercrime victims involves assessing both the financial benefits and the costs associated with implementing and running the service.

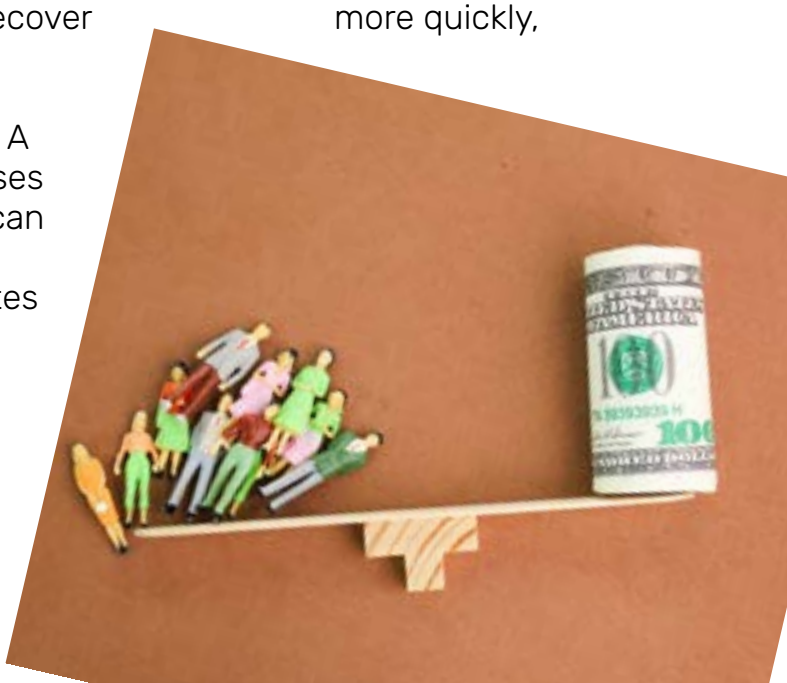
Here is a breakdown of these components.

FINANCIAL BENEFITS

a. Reduced Employee Productivity Loss: Cybercrime incidents can significantly impact employee productivity as they cope with the aftermath. A counselling service can help employees recover more quickly, reducing the time taken off work.

b. Lower Turnover and Recruitment Costs: A supportive work environment that addresses the psychological impact of cybercrimes can contribute to employee satisfaction and retention, potentially lowering turnover rates and associated recruitment costs.

c. Enhanced Reputation and Customer Trust: For businesses, providing



counselling services to their customers affected by cybercrimes can enhance the company's reputation and build trust. This can lead to increased customer loyalty and retention.

COST OF IMPLEMENTING AND OPERATING THE SERVICE

a. Counsellor Salaries and Training: The cost of hiring and training licensed counsellors with expertise in both mental health and cybercrimes.

b. Technology Infrastructure: Developing and maintaining a secure and user-friendly platform for remote counselling sessions.

c. Marketing and Outreach: Costs associated with marketing campaigns to promote the service and educate the target audience about its availability.

d. Operational Overheads: General operational expenses, including administrative costs, legal compliance, and ongoing platform maintenance.

If you are using an external service, then you will only have the cost of the service plus the cost of your internal campaigns to advertise the service.

ROI CALCULATION

Return On Investment (ROI) is calculated as follows:

$$ROI = \frac{\text{(Financial Benefits - Cost of Investment)}}{\text{Cost of Investment}} \times 100$$

a. Net Financial Benefits
Calculate the sum of the financial benefits (reduced productivity loss, lower turnover costs, and enhanced reputation) minus the costs associated with implementing and operating the service.

b. Cost of Investment:
Sum all costs related to counsellor salaries, training, technology infrastructure, marketing, and operational overheads.

c. Example of a simplified calculation:
Let's consider as an example a company of 1,000 employees, with mixed part-time and full-time contracts.

Assumptions:

- We will consider that 9% of these have been victims of identity theft and this is causing them a 35% loss in productivity for their worked hours over the year.

- We will calculate the cost associated to those unproductive hours for the company based on the standard values of $340/day for full time-workers and $170/day for part-time workers.

- We will then estimate that each employee will need 4 hours of counselling as an average and that, conservatively, the efficacy of the counselling session will be 50%.

Calculations:

- Company's employees: 1,000
- Estimated subscribers: 1,000 x 9% = 90
- Full time subscribers: 80
- Part time subscribers: 10
- Full time working hours in a year: 2,080
- Part time working hours in a year: 1,040
- Unproductive hours/year (full-time): 80 x 2,080 x 35% = 58,240
- Unproductive hours/year (part-time): 10 x 1,040 x 35% = 3,619
- Unproductive work cost estimate: (58,240 + 3,619) / 8 x $340 = $2,629,007
- Estimated success rate for the service: 50%
- Estimated savings to the company in one year: $1,314,503
- Hours of sessions x subscribers = 4 x 90 = 360
- Estimated cost of the service = $200,000

ROI = (1,314,503 - 200,000) / 200,000 x 100 = 557 %

A positive ROI of 557% indicates that for every dollar invested in the counselling service, the company gains $5.57 in net financial benefits.

NEGATIVE PID

VII. Advantages of cybercrime victim support for corporations and small businesses

Cybercrime victim support provides significant advantages for both corporations and small businesses.

FOR CORPORATIONS

For corporations, a robust support system helps mitigate the potential negative impacts of cyber incidents on employees.

Swift and effective assistance for victims of identity theft or cyber attacks fosters a sense of security and well-being amongst the workforce, leading to increased morale and productivity.

Additionally, offering counselling services contributes to employee retention and loyalty, as the organization demonstrates a commitment to the well-being of its staff.

FOR SMALL BUSINESSES

For small businesses, cybercrime victim support is equally crucial.

Smaller enterprises may face disproportionately severe consequences from cyber incidents, making employee support paramount.

Prompt resolution of identity theft issues and the provision of counselling services not only aid in maintaining a resilient workforce but also enhance the overall reputation of the business.

In both cases, a supportive framework underscores a proactive approach to cybersecurity, fostering a culture of resilience and preparedness within the organization.

VIII. Implementing cyber crime victim support with Negative PID

At Negative PID we distinguish ourselves from other companies for our cross-disciplinary approach to resolving issues. We believe that a complex problem like cybercrime requires solutions for your technical environment and your human environment.

This is why we have designed a service that combines our cybersecurity experience and human sciences to deliver a **turn-key service** to help you **prevent, remediate, and recover** from cybercrime.

Our unique **CyberCrime Victim Support (CCVS) Teams** are qualified to offer counselling that specifically addresses emotional distress caused by cybercrime incidents.

Our professionals are licensed in the following areas:

- Canada
- US
- UK
- Italy

And we can further expand to different areas upon request, at no additional cost.

Our services can be used by small companies and corporations alike, through a model that scales with your needs.

You can access our services:
- Directly
- Through your group insurance
- Through your cybersecurity insurance company

WHY NEGATIVE PID

Our Cybercrime victim support service has some unique advantages:

- Your employees can use the service in complete privacy: we will maintain their anonymity, while providing you with periodic utilization metrics and feedback based on surveys on the service.

- We provide you with campaign materials for your internal use that are ready to be customized and sent out to your employees.

- Our booking portal will give your employees direct access to the service. From here, they will be able to choose their counsellor of preference within their region, in different languages.

- Their health information will stay with their counsellor, securely stored, and won't be shared with anyone else, granting their total confidentiality.

- Our offer is scalable and viable for small companies and large companies alike: it can be purchased in blocks of hours that you decide how to use: you can allocate a maximum number of hours per employee, or you can leave the pool open until completion.

- There is virtually no lead time for onboarding: sign up for the service on our website and you'll be ready to go in 24 hours.

NEGATIVE PID

- There are no additional fees: the price you pay for the pool of hours includes all the services.

Empower Your Team, Secure Your Future: Invest in Cybercrime Victim Support Services Today!

In an era of escalating cyber threats, safeguarding your organization extends beyond just digital defences.

Prioritize the well-being of your employees with our comprehensive Cybercrime Victim Support Services. By investing in this essential resource, you not only protect your team from the devastating effects of identity theft and cyber attacks but also fortify the very foundation of your business.

Why Choose Our Services:

- Holistic Support: Provide your employees with expert guidance and counselling to navigate the challenges of cybercrime victimization.
- Productivity Enhancement: Swift resolution of identity theft issues minimizes unproductive work hours, ensuring your team remains focused and efficient.
- Employee Retention: Demonstrate a commitment to your workforce's well-being, fostering loyalty and a positive workplace culture.
- Financial Resilience: Mitigate potential financial losses by addressing cybercrime consequences proactively.

Take Action Now: Cyber threats are ever-evolving, and preparedness is key. Ensure your organization's resilience by incorporating Cybercrime Victim Support Services into your cybersecurity strategy.

Don't just defend against attacks – empower your team to overcome them.

Contact us today to learn more and make a proactive investment in the security and well-being of your workforce.

Secure your team, secure your future. Act now!

https://negativepid.com