CybelAngel

WHITE PAPER

How to Manage Third-Party Digital Risk

TABLE OF CONTENTS

Digital Risk is Shifting

Introduction

Cybersecurity is nearly a half century old. Its inauspicious start was a computer worm invented by Bob Thomas, who also invented email. In 1971, the 'Creeper' worm traveled from terminal-to-terminal printing the message, "I'M THE CREEPER: CATCH ME IF YOU CAN." Then, in 1988, a teenager named Robert Morris, Jr., authored the 'Morris Worm.' Unlike its predecessor, the Morris worm accidentally caused outages and crashes on infected machines. The worm spread far enough to spark the first prosecution by the US federal government for the Computer Fraud and Abuse Act (CFAA). This was just the beginning.

By the early 1990s the number of malware samples had grown to tens of thousands. From then until now, the number of identified malware samples has continued to grow exponentially. By some estimates, there are now over 2 billion malware variants introduced to the wild each year.

In response, cybersecurity professionals developed tools, processes, procedures, and training to protect their companies' valuable assets inside their corporate perimeter including: customer and employee PII (personally identifiable information), financial data, intellectual property, etc. This fortress model protects from outside intrusion, but does not address when sensitive data leaves the corporate perimeter.

The adoption of digital transformation, cloud computing, and outsourcing of physical IT infrastructure streamlined processes and lowered costs; however an unintended consequence is enterprise digital assets are now in the hands of *third, fourth*, and *Nth* parties — far outside the corporate security perimeter.

Enterprise digital assets are now in the hands of third, fourth, and Nth parties — far outside the corporate security perimeter.

What is happening outside the enterprise's perimeter and infrastructure requires the same discipline and vigilance applied for decades protecting inside the perimeter. This is particularly critical, given the average number of parties with whom an enterprise shares sensitive information is 583.[1] Addressing data breaches outside your company is vital to managing your third-party digital risk.

[1] Ponemon Institute

According to the Ponemon Institute's recent survey, "53% of organizations have experienced one or more data breaches caused by a third party, costing an average of $7.5 million to remediate."[2] This is just the beginning of the damage.

Enterprises must address third party risk or face the loss of hundreds of millions in third party data breaches. The legal and regulatory consequences of leaked data often includes potential fines and penalties (see chart: *Major Third-Party Data Breaches*). However, these losses pale in comparison to the loss of brand reputation, as acquisition cost and lifetime customer value are both negatively impacted by breaches. It can take years to recover shareholder value and can cripple small companies.

Third-Party Digital Risk

Exchanging information with organizations is the lifeblood of business; however, once data has left your hands, it takes its own journey through your third parties and their suppliers, and so on. It is moved, copied, modified, forwarded, copied once again. It is widely distributed beyond your enterprise perimeter, your visibility, and your controls.

This supply chain journey increases the risk of your data being exposed and/or stolen. Why? There is a myriad of reasons, but some are simple math. Sharing sensitive data with an average of 583 third parties spreads your data over a much larger cyber attack surface, thus increasing the probability of a data leak.

Your data is further exposed when third parties store your data on a cloud storage device, upload the data to an app, or have a contractor work with your data. The odds of a data breach occurring grows with each additional share of the data.

But your company has invested in the developed of third party audit processes and procedures to ensure your suppliers, vendors, and partners implement strong information security to protect your critical data to include: destruction of documents, encryption of data at rest, etc. While these measures are part of a robust third-party risk program, these can give organizations a false sense of security.

Forward-thinking CISOs know that a 360° third-party program must include digital risk protection. It requires constant and comprehensive monitoring for third-party data leaks beyond the corporate perimeter to protect their company from a data breach.

The average number of parties with whom an enterprise shares sensitive information is...

583

[2] Ponemon Institute Cost of a Data Breach report

Estimated direct cost of major data breaches

$152 /RECORD GLOBALLY | $242 /RECORD IN THE U.S.

According to the Ponemon Institute Cost of a Data Breach Report

Major Third-Party Data Breaches Jan 2019 - Mar 2020

DATE	COMPANY	3RD PARTY	BREACHED DATA
MAR 2020	T-Mobile	Email vendor	~1million customers & employees PII **Second security breach in 6 months**
FEB 2020	General Electric	Third-party computer systems and network provider	~205,000 employee passports, birth certificates, drivers' licenses, etc. **Pending employee class action suit (APR 2020)**
FEB 2020	MGM Resorts	Delivery company	142 million guests' information **Multiple class action suits filed**
OCT 2019	LifeLabs	Cloud data server	15 million Canadians Re**ported $1 billion in class action lawsuit**
JUN 2019	Quest Diagnostics	Billing vendor	11.9 million patient records **Billing vendor filed bankruptcy and Quest settled class action suit**
APR 2019	Facebook	Digital Media Company	540 million user IDs and passwords **Estimated over $1 billion in losses**
MAR 2019	Capital One	Cloud data server	>100 million customers **Estimated $300 million in losses**
JAN 2019	Marriott	3rd party software	5.2 million guests' information **Estimated $126 million in losses**

Third-Party Security Incidents Rising

While the above chart identifies the source or cause of the data breach, the type of data lost factors significantly in the incident response and the business impact.

In August 2020, the CybelAngel Analyst Team carried out an analysis of third-party data leaks. The Team examined a dataset of 50 businesses over an 11-month time period from September 2019 to July 2020, including organizations of different sizes, verticals, and geographical areas. The Team sourced 3,981 publicly-accessible (e.g., open servers and databases, cloud applications), data leak incidents with priority levels from minor to critical — all potentially business impacting to the 50 companies in the study.

Across the entire spectrum of data leaks, the data showed **third parties** played an integral role in the following:

- 62% of all Critical Level Incidents
- 93% of leaked documents from unprotected file servers
- 39% of all code data leaks; all of these were caused by negligence (e.g., misconfigurations), and in 81% of cases it was a company's supplier

The following are two anonymized case studies describe how two enterprises experienced a third-party data leak. Then, we will examine how CybelAngel helped each to ensure these data leaks did not become major data breaches.

62% **of all Critical Level Incidents involved third parties**

AUTOMOTIVE CASE STUDY

Vertical: International Automotive Company
Size: >10,000 employees
Geography: European Union

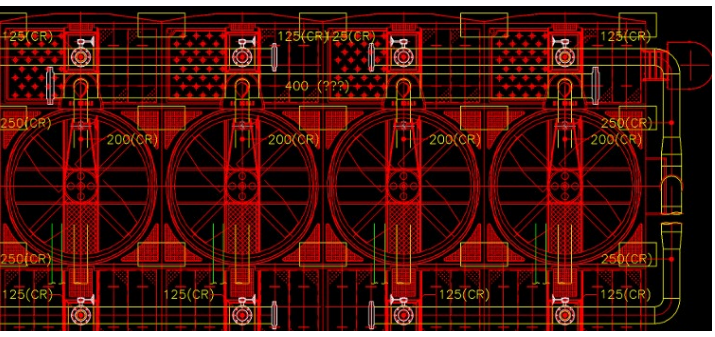
R&D Efforts Were Exposed in the Wild

Problem Description:

This client was working on an important Research & Development (R&D) project with a partner. The company had publicly announced their new product but kept the specifics top secret. If trade secrets were exposed, it would remove the company's first-mover advantage. The result would likely be in the tens of millions of losses, as the R&D program would be obsolete.

Only a small product team including contractors from a trusted partner had knowledge of the technology specifics and launch plans. One of these contractors took work home over the weekend to accelerate progress. What followed was an accidental data leak.

Wanting to be efficient, the contractor plugged his USB key to his home router and created a cloud storage container without a password. The result? Anyone could access the USB and its contents.



Research and Development CAD Drawing

How CybelAngel Protect the Client:

CybelAngel protects our customers by continuously scanning hundreds of thousands of data sources across the internet for publicly-accessible, leaked documents. It was during such a scan that we discovered documents related to this new product and its launch.

Our solution immediately detected leaked documents, which were processed through our Machine Learning algorithms applying a first sensitivity screening and predicting a critical incident. This prediction triggered an alert, which our Analyst Team investigated, until they could precisely identify who was responsible for the leak.

This process enabled the CybelAngel Analyst Team to confirm the criticality of the documents and share this information within minutes of detection. The incident report provided context and details about what was exposed, which helped our client to assess the company's risk and take immediate action. The contractor was contacted and instructed to unplug his USB key and shut down the cloud storage.

CybelAngel continued to monitor for detection of these documents across the Internet — ensuring that no one accessed and leaked the USB content.

RETAIL CASE STUDY

Vertical: Retail
Size: >13,000 employees
Geography: N. America

It's All About Your Customers' PII

Problem Description:

In this case study, a multinational marketplace selling consumer goods used buying behavior data to increase usage of its new rewards program. The company engaged a marketing agency to handle promotion of the digital rewards program and the associated platform.

Customers logged onto the new platform, where the agency linked to the buyer's profile using a database extract provided by our client.

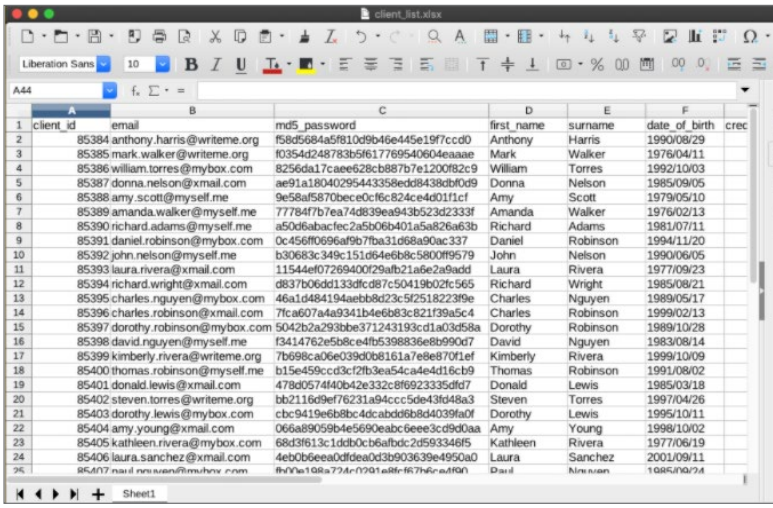
The rewards program went well — it increased customers satisfaction and loyalty scores; however, there were unintended consequences.

Two months into the project, the marketing agency's IT department carried out a migration of its services to new hardware. Unfortunately, some data was left on the old server, including our client's database extract of buyer's behavior. Our client's customer data was now unprotected and publicly exposed. Should this data leak turn into a major breach, the company faced potential CCPA (California Consumer Privacy Act) punitive actions, lawsuits, as well as a loss of its customers' trust.

How CybelAngel Protected the Client:

CybelAngel detected the open server and the database extract only a few days after the agency's services migration. Fortunately, an audit of the marketing agency's network revealed that no other IP had connected to the unprotected server, except the CybelAngel tools.

Closing the data leak before being discovered and exploited by hackers, saved an average of $242 USD per record or an estimated quarter of a billion dollars in losses.



client_id	email	md5_password	first_name	surname	date_of_birth
85384	anthony.harris@writeme.org	f58d5684a5f810d9b46e445e19f7ccd0	Anthony	Harris	1990/08/29
85385	mark.walker@writeme.org	f0354d248783b5f617769540604eaaae	Mark	Walker	1976/04/11
85386	william.torres@mybox.com	8256da17caee628cb887b7e1200f82c9	William	Torres	1992/10/03
85387	donna.nelson@xmail.com	ae91a180402954433 58edd8438dbf0d9	Donna	Nelson	1985/09/05
85388	amy.scott@myself.me	9e58af5870bece0cf6c824ce4d01f1cf	Amy	Scott	1979/05/10
85389	amanda.walker@myself.me	77784f7b7ea74d839ea943b523d2333f	Amanda	Walker	1976/02/13
85390	richard.adams@myself.me	a50d6abacfec2a5b06b401a5a826a63b	Richard	Adams	1981/07/11
85391	daniel.robinson@mybox.com	0c456ff0696af9b7fba31d68a90ac337	Daniel	Robinson	1994/11/20
85392	john.nelson@myself.me	b30683c349c151d64e6b8c5800ff9579	John	Nelson	1990/06/05
85393	laura.rivera@xmail.com	11544ef07269400f29afb21a6e2a9add	Laura	Rivera	1977/09/23
85394	richard.wright@xmail.com	d837b06dd133dfcd87c50419b02fc565	Richard	Wright	1985/08/21
85395	charles.nguyen@mybox.com	46a1d484194aebb8d23c5f2518223f9e	Charles	Nguyen	1989/05/17
85396	charles.robinson@xmail.com	7fca607a4a9341b4e6b83c821f39a5c4	Charles	Robinson	1999/02/13
85397	dorothy.robinson@mybox.com	5042b2a293bbe371243193cd1a03d58a	Dorothy	Robinson	1989/10/28
85398	david.nguyen@myself.me	f3414762e5b8ce4fb5398836e8b990d7	David	Nguyen	1983/08/14
85399	kimberly.rivera@writeme.org	7b698ca06e039d0b8161a7e8e870f1ef	Kimberly	Rivera	1999/10/09
85400	thomas.robinson@myself.me	b15e459ccd3cf2fb3ea54ca4e4d16cb9	Thomas	Robinson	1991/08/02
85401	donald.lewis@xmail.com	478d0574f40b42e332c8f6923335dfd7	Donald	Lewis	1985/03/18
85402	steven.torres@writeme.org	bb2116d9ef76231a94ccc5de43fd48a3	Steven	Torres	1997/04/26
85403	dorothy.lewis@mybox.com	cbc9419e6b8bc4dcabdd6b8d4039fa0f	Dorothy	Lewis	1995/10/11
85404	amy.young@xmail.com	066a89059b4e5690eabc6eee3cd9d0aa	Amy	Young	1998/10/02
85405	kathleen.rivera@mybox.com	68d3f613c1ddb0cb6afbdc2d5933465f5	Kathleen	Rivera	1977/06/19
85406	laura.sanchez@xmail.com	4eb0b6eea0dfdea0d3b903639e4950a0	Laura	Sanchez	2001/09/11

Sample Database with Customers' PII

Decrease Your Third-Party Risk

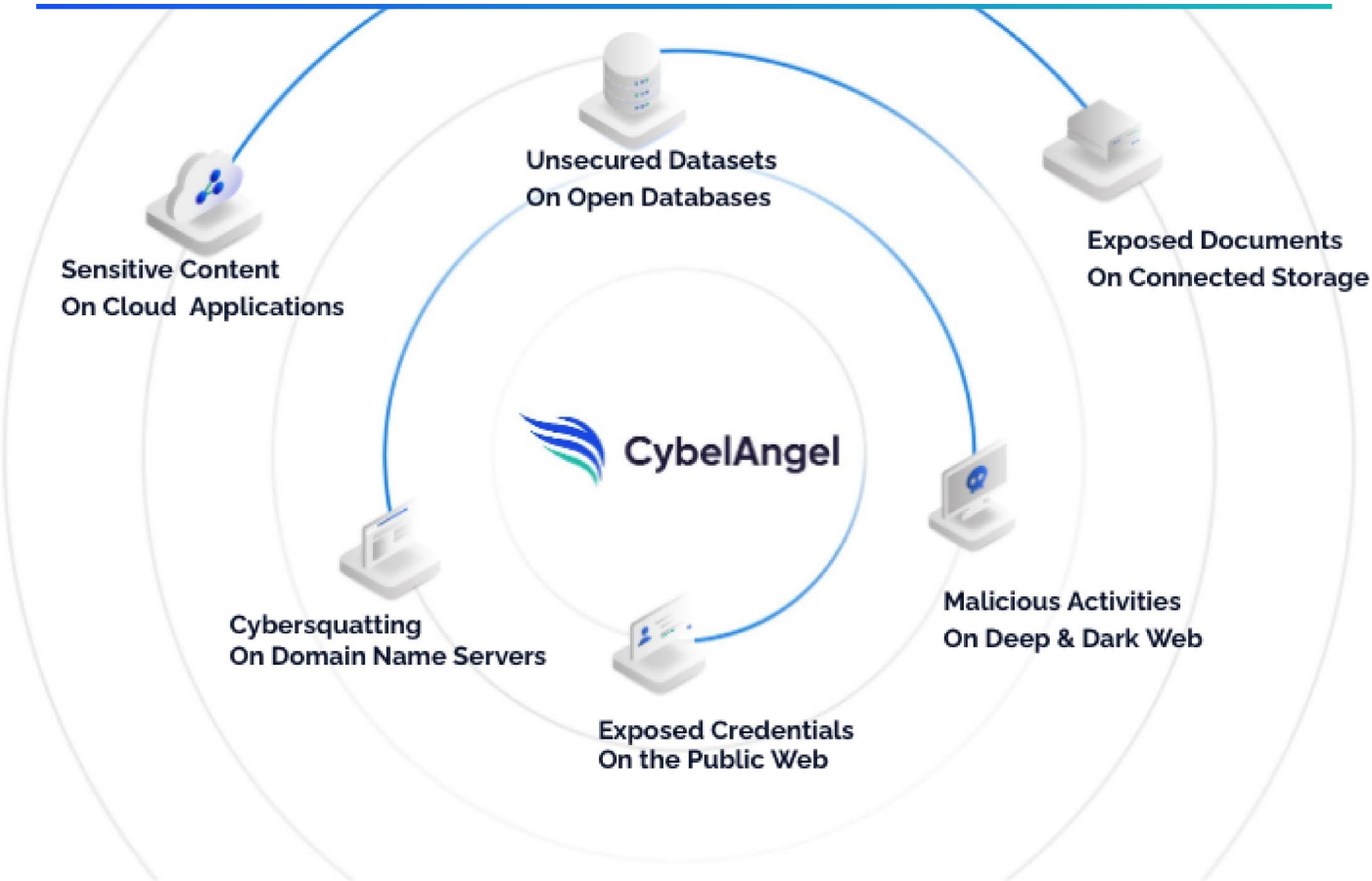
Enterprises need a solution that complements their third-party compliance and governance processes and procedures. The CybelAngel digital risk protection platform fulfills these expectations by expertly executing on three key success factors.

1. Comprehensive scanning outside of your enterprise perimeter is integral to detecting data leaks. This scanning must include: surface web, deep & dark web, domain name servers, cloud applications, connected storage, and open databases and datasets.

2. Speed to detect is critical. Finding confidential and/or sensitive data before it is stolen and exploited is key to a strong digital risk solution.

3. Timely alerting is key. Comprehensive scanning means having to sort, filter, and identify the most critical alerts. Machine learning algorithms funnel the hundreds of thousands of data sources, thousands of files, and hundreds of threats to derive a manageable number. These threats can then be prioritized by cyber experts, who eliminate any false positives and prioritize those potential data leaks that are most likely to become major breaches.

CybelAngel Scans for Sensitive Data Across Key Internet Perimeters



Third-Party Balancing Act

The secure storage, transmission, and accessibility of data is the foundation information security, and effective risk management is essential for a company's ability to remain competitive, profitable, and stable. It is a delicate balancing act, and the addition of the third-party vector adds significant and unexpected weight to risk calculations," said Alex Heid, Chief Research Officer of SecurityScorecard.

"Cybercriminals will often exploit poorly secured third-party service providers as an easy way to hit 'many birds with one stone.' While an established company may have strong defenses in place to guard their local resources, it is easier for an attacker to go after a service provider to that company in order to gain a foothold within the enterprise resources. Furthermore, once an attacker has successfully breached a third-party service provider, the attacker will now have access to resources of EVERY enterprise that relies on that third party.

SecurityScorecard has found that inviting your third-party suppliers to view their own security score leads to an average 7-8 point increase in their cybersecurity rating. Collaboration and communication with third-parties that handle critical services is key, and can be accomplished through the sharing of information between organizations. When businesses are helping each other identify and take action on areas of mutual risk exposure, it can create a 'flywheel effect' that gains momentum and perpetually drives better cyber resilience throughout the entire business ecosystem."

Alex Heid
Chief Research Officer SecurityScorecard and CybelAngel Partner

CybelAngel enables companies to protect against data leaks becoming devastating breaches, regardless of where the data lives. We use advanced machine learning to detect leaks of customers' sensitive data, whether these occur on third-party servers or in cloud storage.

Our data leak platform scans for confidential and proprietary data and its location, instantly alerting our clients when their sensitive data is at risk. To fix data leaks, our clients take action internally or rely on CybelAngel's security experts to resolve the risk.

Do you know the scope of your organization's data leaks risk? CybelAngel will provide you a dashboard that indicates where your company's data is leaking and how you rank compared to other organizations in your industry — without any obligation.

Click here to get your company's complimentary Data Leak Dashboard.

If you suspect a data leak, **Chat with an Expert.** Because data leaks are inevitable, but damage is optional.

Do you know your organization's risk for data leaks?

CLICK HERE to get your company's Data Leak Dashboard.

About CybelAngel

CybelAngel reduces global enterprise digital risk by detecting critical data leaks outside the firewall before these leaks become major data breaches. Leveraging its Augmented Intelligence, a unique combination of proven machine learning capabilities and superior cyber analysts, CybelAngel analyzes billions of data sources, thousands of files, and hundreds of threats across all layers of the internet to discover critical data leaks for their customers. Global organizations rely on CybelAngel every day to detect critical data leaks before wreaking havoc on their business.

Learn more at www.cybelangel.com