



PROGRAM MATERIALS

Program #3134

February 23, 2021

Lessons in Disaster: Learning from Law Firm Cyber Breaches

Copyright ©2021 by

- **Mark Sangster - Author of “No Safe Harbor” and eSentire VP Industry Security Strategies**

**All Rights Reserved.
Licensed to Celesq®, Inc.**

Celesq® AttorneysEd Center
www.celesq.com

**5255 North Federal Highway, Suite 100, Boca Raton, FL 33487
Phone 561-241-1919**



Lessons in Disaster

Learning from Data Breaches

MARK SANGSTER
Cybersecurity author and advocate



[Linkedin/in/mbsangster](https://www.linkedin.com/in/mbsangster)



[@mbsangster](https://twitter.com/mbsangster)



[@cyber_mbsangster](https://www.instagram.com/cyber_mbsangster)



mbsangster.com



mark@mbsangster.com



“Only after disaster can we be resurrected.”



Tyler Durden

Fight Club 1999 Chuck Palahniuk

When we blame the people, we miss the chance to learn
Sidney Dekker, The Field Guide to Understanding Human Error

HUMAN ERROR is never the cause.
It is a symptom of underlying **SYSTEMIC PROBLEMS**



HINDSIGHT bias
The exaggerated ability to predict and prevent the disaster



OUTCOME bias
Knowing the outcome tends to lead to harsh judgment



TIME bias
The tendency to focus on the most recent factors



eSENTIRE

On July 23 1983, Air Canada 143 was a passenger flight between Montreal and Edmonton. Midway through the flight at an altitude of 41,000 feet, the plane ran out of fuel.



On July 23 1983, Air Canada 143 was a passenger flight between Montreal and Edmonton. Midway through the flight at an altitude of 41,000 feet, the plane ran out of fuel.

The crew was able to glide the Boeing 767 aircraft safely to an emergency landing at a former Air Force base in Gimli, Manitoba. There were only minor injuries. This unusual aviation incident earned the aircraft the nickname "Gimli Glider."



Initially hailed as heroes, following the airline's internal investigation, Captain Pearson was demoted for six months and First Officer Quintal was suspended for two weeks for allowing the incident to happen. Three maintenance workers were also suspended.



ACCOUNTABILITY

FAA + NTSB

REGULATORY



CHANGES

GLASS COCKPIT
FLY-BY-WIRE



TWO PILOTS
REDUCED CREW



NOVEL
AIRCRAFT DESIGN



EMERGING
TECHNOLOGY



HUMAN ERRORS
MISCALCULATIONS



OBSOLETE
GOVERNANCE



MECHANICAL
FAILURES

AVIATION
THREATS

ACCOUNTABILITY
COMPLIANCE + CONTRACTS



ACCESS
REMOTE WORKERS



HANDS-ON
KEYBOARD



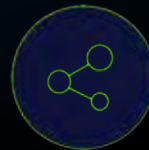
ASSETS
CLOUD-BASES



MALWARE
AS-A-SERVICE



WORKLOADS
DISTRIBUTED



CULTURAL
ENGINEERING



EMERGING
TECHNOLOGY

SOPHISTICATED
THREATS



STATE-SPONSORED actors move down stream
while **ORGANIZED CRIME** grows in ferocity and coordination

1

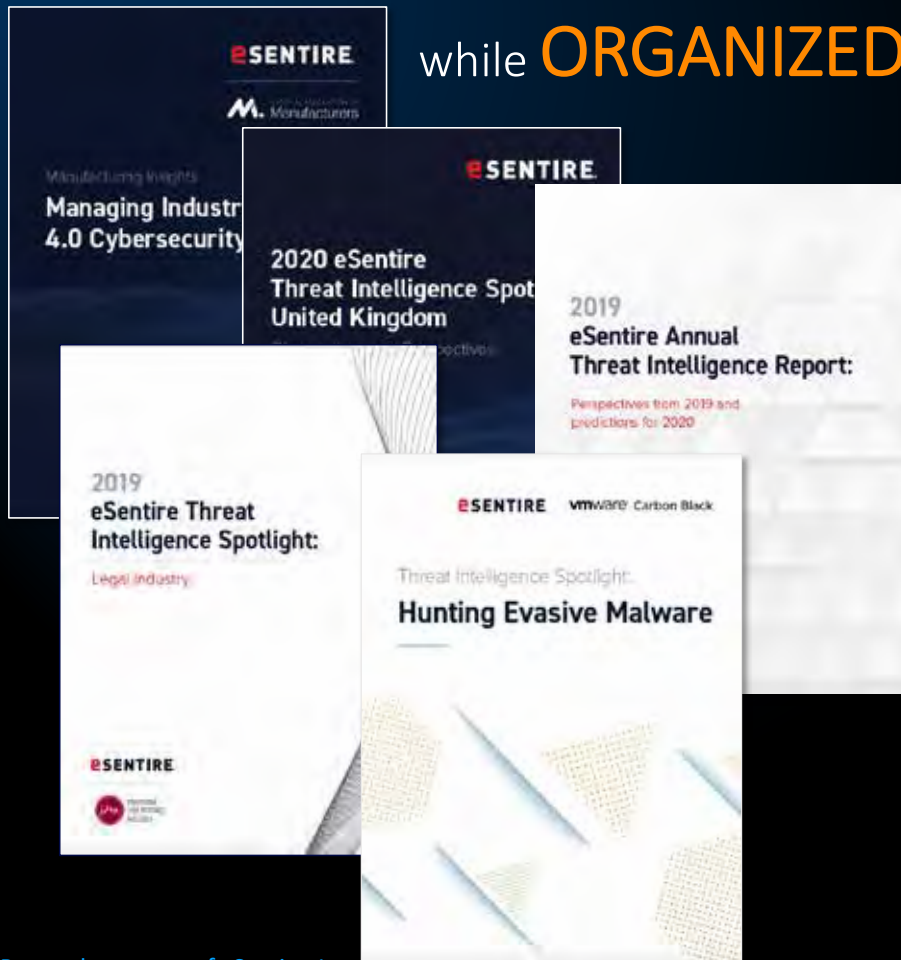
USING YOUR OWN TOOLS
HAND-ON-KEYBOARD

2

F500 BUSINESS PRACTICES
MALWARE AS-A-SERVICE

3

THEY UNDERSTAND YOUR BUSINESS
CULTURE-BASED ATTACKS



Research courtesy of eSentire, Inc.



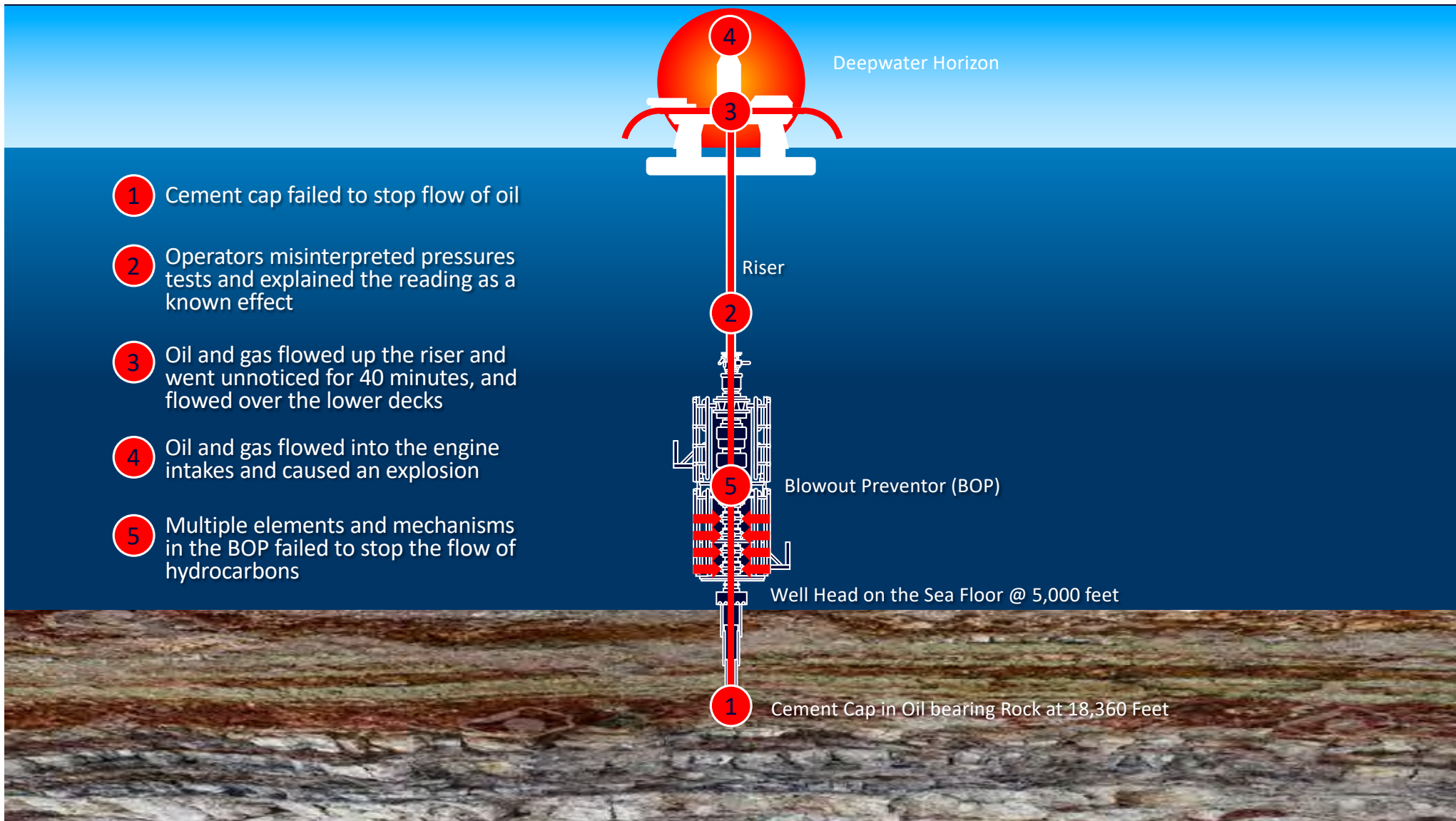
On 23 April 2010, 43 days behind schedule, two massive explosions ripped through the Deepwater Horizon, a \$560 million offshore drilling rig.

While most of the crew escaped with their lives, 11 people were later presumed dead. After 83 days of uncontrolled flow, more than five million barrels of oil led to the largest environmental disaster in history, causing immense damage to the Louisiana coast and Gulf of Mexico.

The estimated cost of this event is somewhere around 65 billion.

Initial investigations pointed to operator error.

<https://vfxblog.com/2016/11/22/ilm-is-on-fire-with-deepwater-horizon/>



ACCOUNTABILITY
USCG + BP + Congress

DRIVERS

BUDGET + SCHEDULE

OPERATOR ERRORS
"BLADDER EFFECT"

CEMENT CAP
Untested Mix

DRILLING DEPTH
UNTESTED METHODS

COMMUNICATIONS
ERRORS / OMISSIONS

SAFETY MECHANISM
FAILED TO FUNCTION

CHAIN OF COMMAND
CONFLICTS

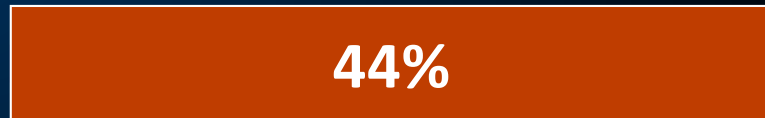
EMERGING
TECHNOLOGY

SUPPLY CHAIN
RISKS

https://en.wikipedia.org/wiki/Deepwater_Horizon_explosion

eSENTIRE

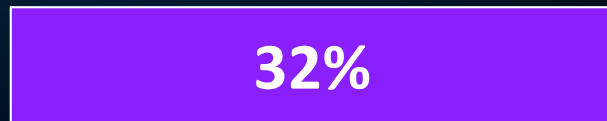
Third-party risk reality



Experienced a third-party material breach



Were notified by the third party responsible



Lack resources to audit third parties



Research courtesy of eSentire, Inc.

Public references



Department of Financial Services

NYCRR 500 Section 11



Supply Chain Security Guidance



The 3Ps of third-party risk

POLICIES

MINIMIZE

1. Define Supply Chain Policies
2. Develop Due Diligence Tools
3. Establish Periodic Validation
4. Raise Security Awareness
5. Encourage Improvement

PREVENTION

MEASURE

1. Identify Assets and Obligations
2. Define Risk Appetite
3. Conduct Risk Assessments
4. Analyze Results and Risks
5. Define Defensive Requirements

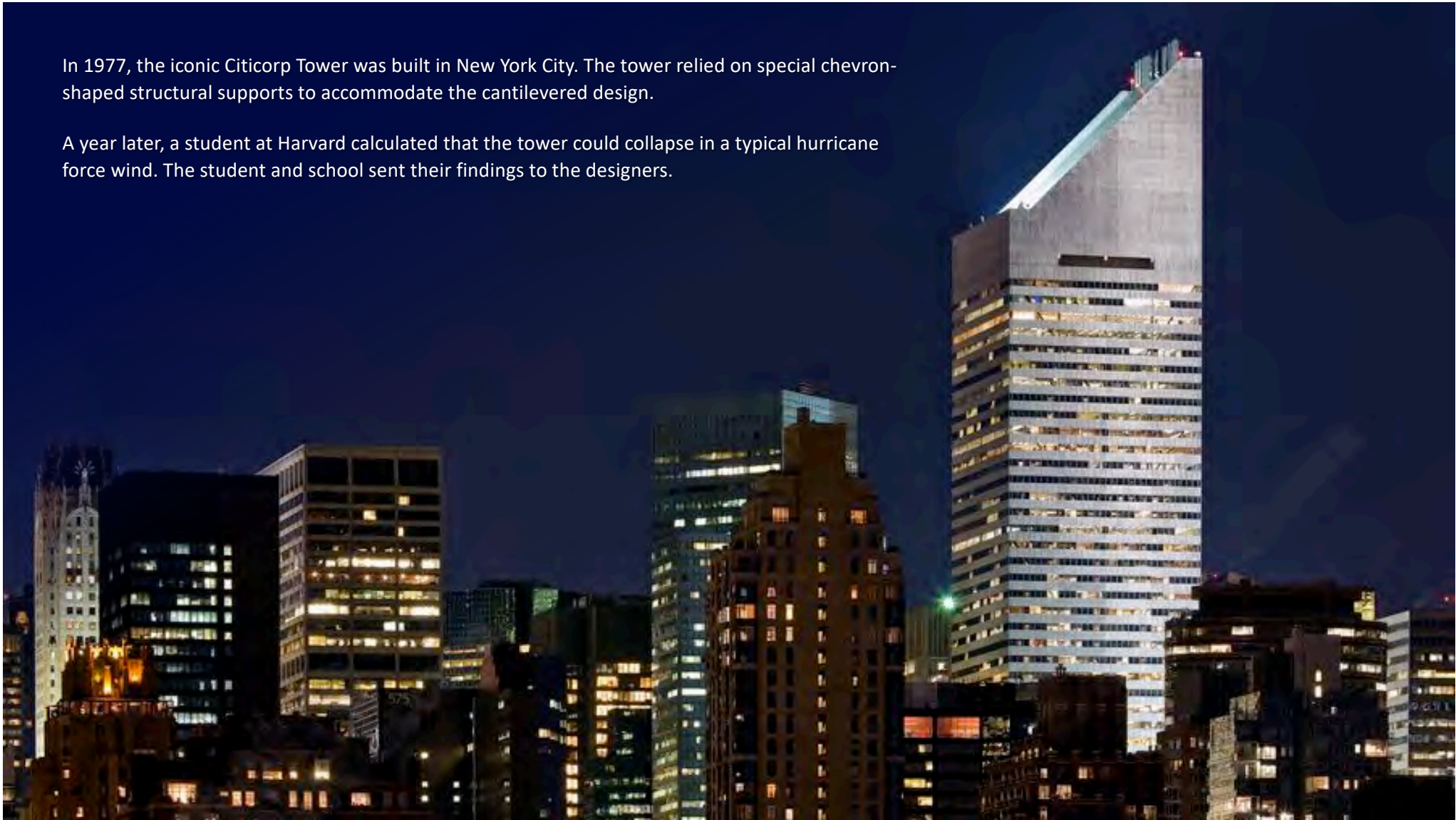
PROMISES

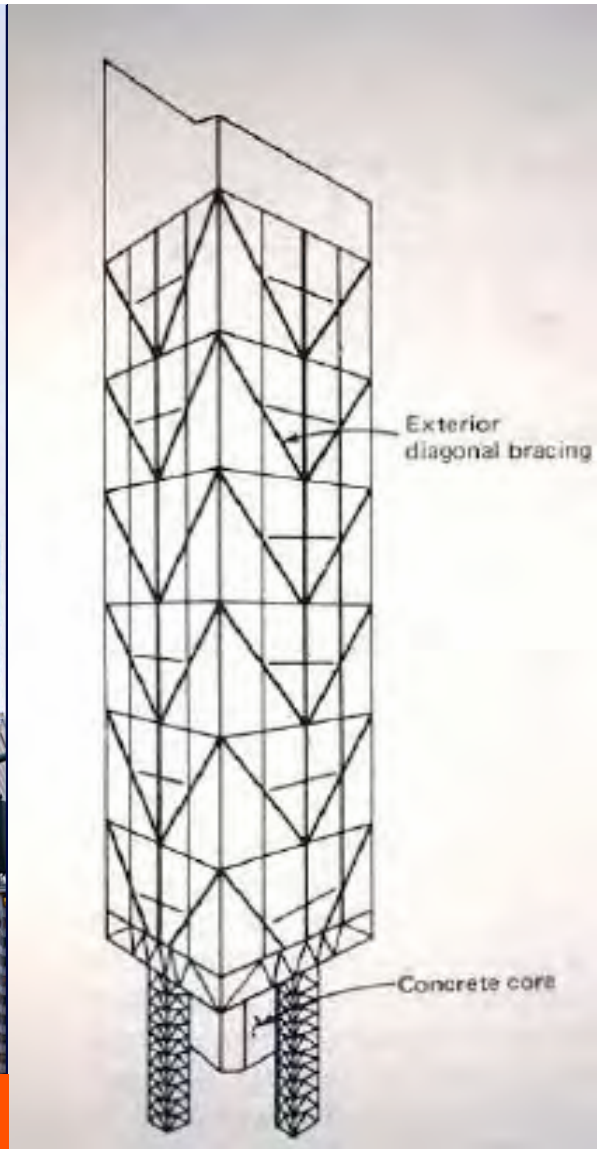
MITIGATE

1. Contractual Obligations
2. Demark Responsibilities
3. Establish Minimum Standards
4. Document Notifications
5. Representations/Warranties

In 1977, the iconic Citicorp Tower was built in New York City. The tower relied on special chevron-shaped structural supports to accommodate the cantilevered design.

A year later, a student at Harvard calculated that the tower could collapse in a typical hurricane force wind. The student and school sent their findings to the designers.



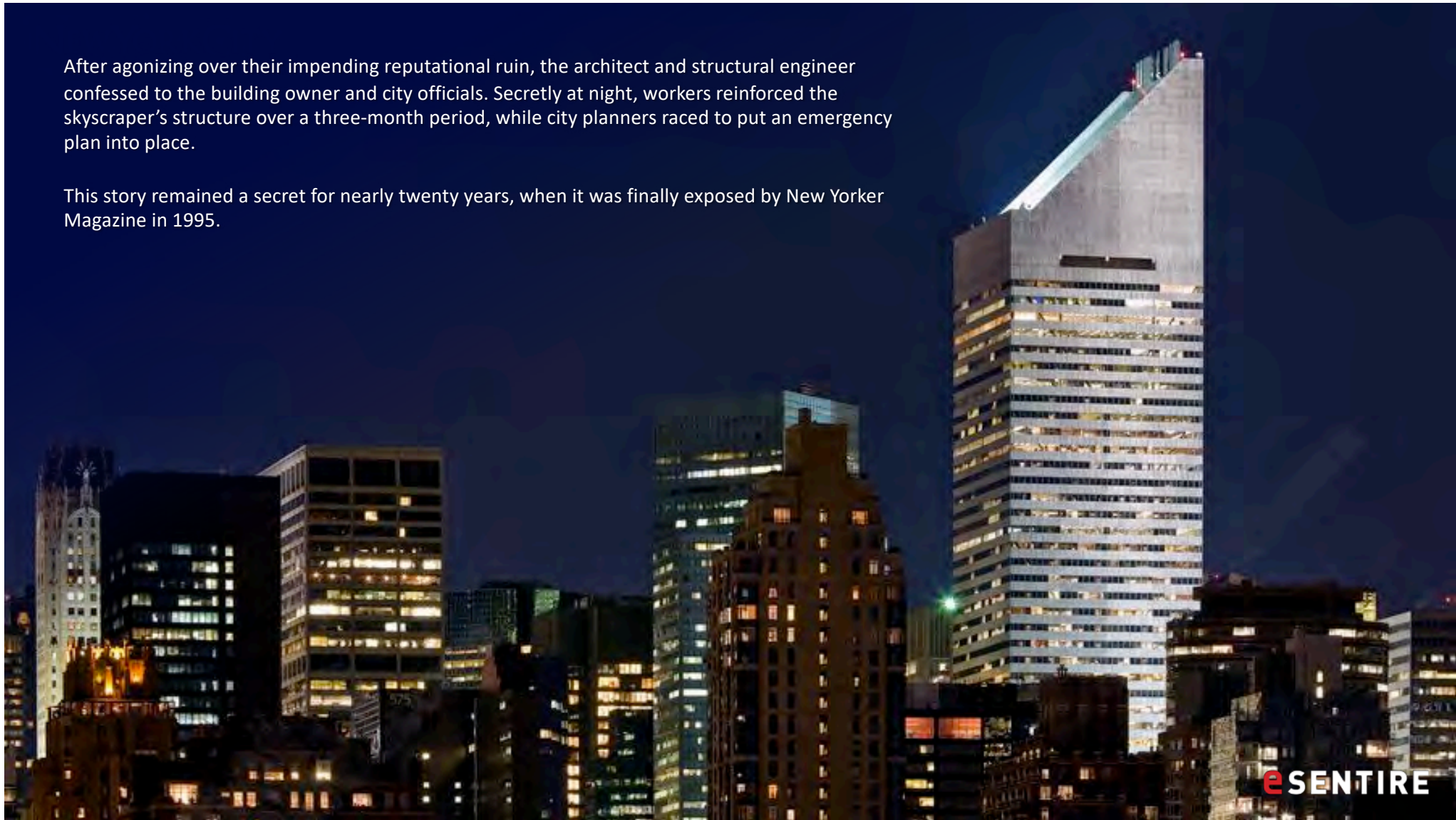


LEFT: <https://amazing.zone/citigroup-center-skyscraper-collapse-averted-by-student-s-phone-call>

RIGHT: <http://www.bobybarra.com/blog/2015/10/16/remarkable-engineering-almost-a-disaster-citicorp-tower-nyc>

After agonizing over their impending reputational ruin, the architect and structural engineer confessed to the building owner and city officials. Secretly at night, workers reinforced the skyscraper's structure over a three-month period, while city planners raced to put an emergency plan into place.

This story remained a secret for nearly twenty years, when it was finally exposed by New Yorker Magazine in 1995.



ACCOUNTABILITY
CITY OF NEW YORK + ARCHITECTS ASSOC.

OBLIGATIONS

ETHICS

BUILDING CODES
INSUFFICIENT

VENDOR CHANGES
BOLTS NOT WELDS

MISLEADING
PUBLIC STATEMENTS

AGREEMENT
CITI BANK + BUILDER

PUBLIC SAFETY
ISSUES

DISCLOSURE
PERSONAL RUIN

EMERGING
TECHNOLOGY

SUPPLY CHAIN
RISKS



Privacy breach - An update on the police investigation

Montreal, November 1, 2019 - On October 31, the Sûreté du Québec informed Desjardins that the privacy breach, which was initially announced on June 20, appears to have affected the data of 4.2 million individual caisse members who do their banking with Desjardins in Quebec and Ontario. There is no information at this time about whether or not more business members have been affected. As a reminder, this situation only involves caisse members who use Desjardins banking services in Quebec and Ontario.

...described the situation as one in which a staffer “shared” personal information of 2.7 million people. (later increased to 4.2 million)

John MacFarlane - CBC News · Posted: Nov 01, 2019 10:44 AM ET | Last Updated: November 1, 2019
Guy Cormier, president and CEO of Desjardins Group, speaks during a news conference in Montreal Friday, explaining the data theft is much larger than first thought. (Ivanoh Demers/Radio-Canada)




MARKETS

Capital One Cyber Staff Raised Concerns Before Hack

Cybersecurity employees reported what they saw as staffing issues and other problems to bank's internal auditors, human-resources department and other senior executives

By AnnaMaria Andriotis and Rachel Louise Ensign

Updated Aug. 15, 2019 6:08 pm ET

 The data breach was tied to the detection of “an outside individual” who was able to get unauthorized access to personal information from Capital One credit card customers.

Before a giant data breach at Capital One Financial Corp., employees raised concerns within the company about what they saw as high turnover in its cybersecurity unit and a failure to promptly install some software to help spot and defend against hacks, according to people familiar with the matter.

The cybersecurity unit—responsible for ensuring Capital One’s firewalls were properly configured and scanning the internet for evidence of a data breach—has cycled through senior leaders and staffers in recent years, according...

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

MARKETS

Capital One Before a giant data breach at Capital One Financial Corp., COF 3.02% employees raised concerns within the company about what they



A LexisNexis Company

Capital One Ordered To Release Report Of Massive Data Heist

Law360 (May 27, 2020, 10:47 PM EDT) -- Capital One Financial Corp. has been ordered to disclose a cybersecurity firm's forensic analysis of its massive 2019 data breach, after a

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE: CAPITAL ONE CONSUMER
DATA SECURITY BREACH LITIGATION) MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to the Consumer Cases

MEMORANDUM OPINION AND ORDER

This matter is before the court on plaintiffs' motion to compel production of Mandiant Report and related materials. (Docket no. 412). Plaintiffs have filed a memorandum in support (Docket nos. 413, 416), Capital One has filed an opposition (Docket no. 435), and plaintiffs have filed a reply (Docket nos. 445, 447). The court heard argument on this motion on May 15, 2020. Having reviewed the pleadings filed by the parties and considered the arguments raised by counsel, and for the reasons stated below, the court finds that Capital One has not carried its burden of establishing that the Mandiant Report is entitled to protection under the work product doctrine.

Background

Capital One entered into a Master Services Agreement ("MSA") with FireEye, Inc., d/b/a Mandiant ("Mandiant") on November 30, 2015, and thereafter entered into periodic Statements of Work ("SOW") and purchase orders with Mandiant pursuant to the MSA. (Blevins Decl. ¶ 4, Docket no. 435-1). As stated by Jeffrey Blevins II, a senior manager of Capital One's Cyber Security Operations Center, "one purpose of the MSA and associated SOW's was to ensure that Capital One could quickly respond to a cybersecurity incident should one occur. As a financial institution that stores financial and other sensitive information, it is critical that Capital One be

to be performed under the direction of external and internal

ation is compelled is granted in part. Capital One shall provide a Report pursuant to the terms of the Protective Order with Local Civil Rule 37(c). Capital One shall have eleven days to file its opposition to plaintiffs' motion to compel "related materials" is denied. Capital One's opposition, the issues concerning all related (Docket no. 435 at 28-30). The parties have not had an opportunity to review related materials and to consider any privilege over related materials and to consider any way may be entitled to be withheld from production even if it is entitled to work product protection.

, 2020.

John F. Anderson
United States Magistrate Judge
John F. Anderson
United States Magistrate Judge

[www.dailymail.co.uk › news › article-7362679 › Capital One employees 'alerted managers of huge data breach 2019'](https://www.dailymail.co.uk/news/article-7362679/Capital-One-employees-alerted-managers-huge-data-breach-2019.html)

Capital One employees 'alerted managers of huge data breach 2019'

Aug 15, 2019 - But before that huge hack, employees of the company came forward with concerns that they were understaffed, there were problems with the ...

The cybersecurity firm's forensic analysis of its massive 2019 data breach—has cycled through senior leaders and staffers in recent years, according to a source familiar with the company's internal communications.



29 JAN 2020 **BLOG**

Why the Travelex Incident Portends the Changing Nature of Ransomware



Mark Sangster VP and industry security strategist, eSentire

Follow @mbsangster Connect on LinkedIn



U.S. DEPARTMENT OF THE TREASURY

Treasury Department Issues Ransomware Advisories to Increase Awareness and Thwart Attacks

Advisories provide guidance and tools to recognize, resist, and report attacks

WASHINGTON—The U.S. Department of the Treasury's Office of Terrorism and Financial Intelligence today

issued a pair of advisories to assist financial institutions in recognizing, resisting, and reporting ransomware attacks, which continue to increase in frequency and severity. The advisories are implemented and enforced by the Office of Foreign Assets Control (OFAC) and the Office of Financial Sanctions Implementation (OFSI). The implications for persons involved in ransomware payments are vital, as ransomware payments are vital to the success of many businesses and can result in significant financial loss and reputational damage.



U.S. DEPARTMENT OF THE TREASURY

Ransomware Advisory

10/01/2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing an advisory to alert companies that engage with victims of ransomware attacks of the potential sanctions risks for facilitating ransomware payments. This advisory highlights OFAC's designations of malicious cyber actors and those who facilitate ransomware transactions under its cyber-related sanctions program. It identifies U.S. government resources for reporting ransomware attacks and provides information on the factors OFAC generally considers when determining an appropriate enforcement response to an apparent violation, such as the existence, nature, and adequacy of a sanctions compliance program. The advisory also encourages financial institutions and other companies that engage with victims of ransomware attacks to report such attacks to and fully cooperate with law enforcement, as these will be considered significant mitigating factors.



FinCEN ADVISORY

FIN-2020-A006

October 1, 2020

Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Detecting and reporting ransomware payments are vital to prevent and deter cybercriminals from deploying malicious software to extort individuals and businesses and hold ransomware attackers accountable for their crimes.

This Advisory should be shared with:

• Chief Executive Officers

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to predominant trends, typologies, and potential indicators of ransomware and associated money laundering activities. This advisory provides information on: (1) the role of financial intermediaries in the processing of ransomware payments; (2) trends and typologies of ransomware and associated payments; (3) ransomware-related financial red flag indicators; and (4) reporting and sharing information related to ransomware attacks.

The information contained in this advisory is derived from FinCEN's analysis of cyber- and ransomware-related Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, the perpetrators threaten to publish sensitive files belonging to the victims, which can be individuals or business entities.

Cybersecurity is not an **IT Problem** to solve...
It's a **Business Risk** to manage.



1
Understand
your role



2
Conduct
awareness training



3
Test Employees
friendly phishing



4
Report
suspicious emails



5
Establish
controls + governance

Leadership: Finding factors not fault

1

AWARENESS

Understand the impact of cyber risks and trends, experiencing business impact of a breach and exposing personal risks

2

RISK

Identifying non-public assets, protected data, and documenting regulatory and contractual obligations

3

PROGRAM

Establishing budget, staffing and programs that align to overall business risk priorities

4

REPORTING

Annual planning, quarterly reporting, dashboards and peer/industry comparisons of performance

5

INCIDENTS

Understanding incident response, board roles, critical business decisions, reporting to authorities and crisis communications



Helping board members get to grips with cyber security



it's a **simplification**... But the case isn't closed. It's barely open. It's time to stop blaming one actor and **look deeper** at the **systemic causes**.



Ask **what** is responsible not **who**



Understand **why** they made their decision



Seek forward **accountability**

NO SAFE HARBOR

THE INSIDE TRUTH
ABOUT CYBERCRIME—
AND HOW TO PROTECT
YOUR BUSINESS

MARK SANGSTER

I can't think of anyone better qualified to tell cybersecurity war stories than Mark. This book is a riveting read, filled with details that people don't normally get to hear about.

Danny Bradbury,
Dark Reading

Mark's book gets to the root causes of why there is no safe harbor for any of us. Each chapter lists practical cyber security steps we should all take – starting today!

Mike StJohn-Green,
Independent Cybersecurity Consultant

Mark's advice could not have arrived at a more propitious moment. The book reads like a collection of short stories, all revolving around a central theme: Cybersecurity is a business risk. This book should be essential reading for senior management and corporate directors.

Kenneth Rashbaum,
Partner, Barton LLP



LinkedIn/in/mbsangster



@mbsangster



@cyber_mbsangster



mbsangster.com



mark@mbsangster.com