Don’t Get Fired!

Financial lessons from the United Health,
NPD, Stoli Group USA, Blackbaud & Clorox incidents

Goals For Today

1. Learn about recent cybersecurity events
2. Understand financial impact for publicly traded + private companies
3. Tell better stories!

TAKEAWAYS: Specific action items for cyber leaders and sales professionals

We’re going to be moving fast. Contact me if you want slides.

About Me

Jay Bobo
github.com/jaybobo

Building security products and securing web applications

- 25 years in tech (B2B/B2C)
- 10 years in healthcare
- 7 years in product security

Scan this.
Talk about this.
Worry about this.

Ignore this.

“CISOs need to translate the cybersecurity request for funds into the language of the rest of the organization”

— Doug Hubbard, author of “How to Measure Anything in Cybersecurity”

Source: https://www.youtube.com/watch?v=bYjPmptlc14

“The human mind is a story processor, not a logic processor.”

— Jonathan Haidt

Let’s get into it…

United Healthcare

Change Healthcare Incident
February 2024

Overview: United Healthcare

- UnitedHealthcare Group is a Fortune 10 (NYSE: UNH)
  - Optum is the largest employer of physicians in the country
  - Change is the 2nd largest switch in the US with approx 20% of the market.
- February 21, 2024 - They experienced a ransomware attack
- February 22, 2024 - They notified the SEC and general public

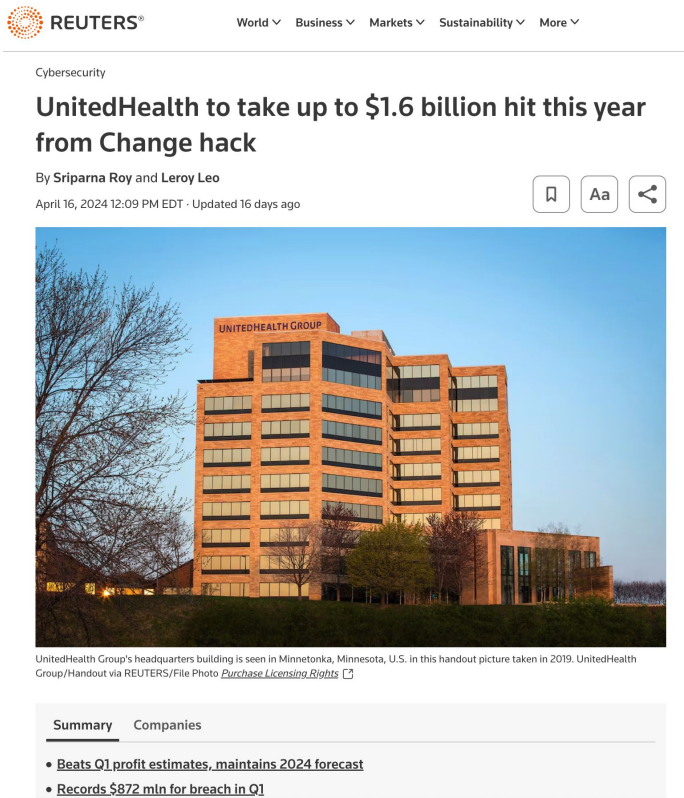

USD
UnitedHealth Group Incorporated · 1D · NYSE
O474.00 H481.19 L473.6
490.82
0.00
490.82
SI ⌀ 5.102M
536.00
532.00
528.00
523.48
520.00
516.00
512.00
508.00
504.00
500.00
496.00
490.82
488.00
484.00
480.00
475.91
472.00
468.00
464.00
523.48
Feb 26:
The media picks up on
story (Monday).
Feb 22
SEC 8-k notification
Feb 21
Initial network Interruption
Notification to customers
Feb 28:
Alphv/Blackcat confirms
the attack on dark web.
Mar 6:
$523 to $472
10% drop in price
472.53
14

Impact: UHG

April 16, 2024

United releases Q1 results and estimates full year 2024 impacts of $1.15 to $1.35 per share which included direct response efforts and business disruption **(~$1.6 billion)**.

- $375mm is estimated to be Change Healthcare directly.
- **YoY revenues for Q1 were up $8b**



REUTERS® World Business Markets Sustainability More

Cybersecurity

UnitedHealth to take up to $1.6 billion hit this year from Change hack

By **Sriparna Roy** and **Leroy Leo**

April 16, 2024 12:09 PM EDT · Updated 16 days ago

UnitedHealth Group's headquarters building is seen in Minnetonka, Minnesota, U.S. in this handout picture taken in 2019. UnitedHealth Group/Handout via REUTERS/File Photo *Purchase Licensing Rights*

Summary Companies

- Beats Q1 profit estimates, maintains 2024 forecast
- Records $872 mln for breach in Q1

Impact: UHG

May 1, 2024

CEO Witty testified to Congress.

- Use of compromised creds from prior incident
- Access via Citrix portal
- Lack of MFA

- **<u>Up to ⅓ of US population's data impacted</u>**

REUTERS®

World Business Markets Sustainability More

United States

UnitedHealth says hackers potentially stole a third of Americans' data

By **Ahmed Aboulenein** and **Zeba Siddiqui**

May 1, 2024 5:57 PM EDT · Updated 17 hours ago

[1/2] UnitedHealth CEO Andrew Witty testifies before a Senate Finance Committee hearing about a recent cyberattack at the company's technology unit and its impact on patients and providers, in this frame grab taken from video on Capitol Hill in Washington, U.S., May 1, 2024. U.S. Senate/Handout via... *Purchase Licensing Rights* **Read more**

WASHINGTON, May 1 (Reuters) - Hackers who breached UnitedHealth's (UNH.N) tech unit in February potentially stole a third of Americans' data, the largest U.S. health insurer's CEO told a Congressional committee on Wednesday.

Two Congressional panels grilled CEO Andrew Witty about the cyberattack on the company's Change Healthcare unit, which processes around 50% of all medical claims in the U.S.

How Much Did It Hurt?

Summary of our Major Sources and Uses of Cash and Cash Equivalents

(in millions)	For the Years Ended December 31, 2023	2022	2021	Change 2023 vs. 2022
Sources of cash:				
Cash provided by operating activities	$ 29,068	$ 26,206	$ 22,343	$ 2,862
Issuances of long-term debt and short-term borrowings, net of repayments	4,280	12,536	2,481	(8,256)
Proceeds from common share issuances	1,353	1,253	1,355	100
Customer funds administered	—	5,548	622	(5,548)
Cash received for dispositions	685	3,414	15	(2,729)
Total sources of cash	35,386	48,957	26,816	

$35 billion in cash.

How Much Did It Hurt?

Financial Condition

As of December 31, 2023, our cash, cash equivalent, available-for-sale debt securities and equity securities balances of $75.2 billion included $25.4 billion of cash and cash equivalents (of which $1.3 billion was available for general corporate use), $44.9 billion of debt securities and $4.9 billion of equity securities. Given the significant portion of our portfolio held in cash equivalents, we do not anticipate fluctuations in the aggregate fair value of our financial assets to have a material impact on our liquidity or capital position. Other sources of liquidity, primarily from operating cash flows and our commercial paper program, which is fully supported by our bank credit facilities, reduce the need to sell investments during adverse market conditions. See Note 4 of the Notes to the Consolidated Financial Statements included in Part II, Item 8, "Financial Statements and Supplementary Data" for further detail concerning our fair value measurements.

$75.2 billion in cash and investments.

Financial Impact

- Why did UHG claim initially that the event was not material (8-k)?
- Was UnitedHealthcare been truly materially impacted? If not, what are the other controls that minimized cyber risk?
- How does the incident compare to the business impact of similar events?

How Much Did It Hurt (FY24)?

Change Healthcare Cyberattack

As previously announced, on February 21, 2024, we identified that cybercrime threat actors had gained access to certain Change Healthcare information technology systems. Upon detection of this outside threat, we isolated the impacted systems to protect our partners and customers.

We have substantially mitigated the impact to consumers and care providers of the unprecedented cyberattack on the U.S. health system and restored or replaced the majority of the affected Change Healthcare services. To support care providers we provided interest-free loans of more than $9 billion through December 31, 2024. For the year ended December 31, 2024, we incurred $2.2 billion of direct response costs, including costs associated with providing interest-free loans; increased medical care expenditures, as we suspended some care management activities to help care providers with their workflow processes; network restoration; and notifications of impacted persons. Optum Insight also experienced estimated business disruption impacts of $867 million for the year ended December 31, 2024, reflecting lost revenue while maintaining full readiness of the affected Change Healthcare services. We expect to continue to incur direct response costs and experience business disruption impacts at a lesser extent in 2025 as we work to bring transaction volumes back to pre-event levels and win new business.

We have determined the estimated total number of individuals impacted by the Change Healthcare cyberattack is approximately 190 million. The vast majority of those people have already been provided individual or substitute notice. The final number wil be confirmed and filed with the Office for Civil Rights. Change Healthcare is not aware of any misuse of individuals' information as a result of this incident and has not seen electronic medical record databases appear in the data during the analysis. It is possible that future risks and uncertainties resulting from the Change Healthcare cyberattack, including risks related to impacted data, litigation, reputational harm, and regulatory actions could adversely affect our financial condition or results of operations.


HOLD ONTO YOUR BUTTS.

How Much Did It Hurt (FY24)?

$3 billion impact in one year!

(~10% of operating earnings)

UNITEDHEALTH GROUP
EARNINGS BY BUSINESS - SUPPLEMENTAL FINANCIAL INFORMATION
(in millions, except percentages; unaudited)

		Optum				
	UnitedHealthcare	Optum Health	Optum Insight	Optum Rx	Total Optum	UnitedHealth Group Consolidated
Three Months Ended December 31, 2024						
Earnings from operations	$2,973	$1,791	$1,270	$1,739	$4,800	$7,773
Direct response costs - cyberattack	9	—	420	—	420	429
South American impacts	55	—	—	—	—	55
Adjusted earnings from operations (b)	$3,037	$1,791	$1,690	$1,739	$5,220	$8,257
Total direct response costs - cyberattack (c)	$9	$—	$420	$—	$420	$513
Operating margin	4.0 %	7.0 %	26.6 %	4.9 %	7.4 %	7.7 %
Adjusted operating margin (b)	4.1 %	7.0 %	35.3 %	4.9 %	8.0 %	8.2 %
Business disruption impacts - cyberattack (d)	$—	$—	$120	$—	$120	$120
Total cyberattack impacts	$9	$—	$540	$—	$540	$633
Three Months Ended December 31, 2023						
Earnings from operations	$3,122	$1,691	$1,284	$1,592	$4,567	$7,689
Operating margin	4.4 %	6.9 %	26.8 %	5.1 %	7.7 %	8.1 %
Year Ended December 31, 2024						
Earnings from operations	$15,584	$7,770	$3,097	$5,836	$16,703	$32,287
Direct response costs - cyberattack	494 (a)	160 (a)	1,296	—	1,456	1,950
South American impacts	170	—	—	—	—	170
Adjusted earnings from operations (b)	$16,248	$7,930	$4,393	$5,836	$18,159	$34,407
Total direct response costs - cyberattack (c)	$494	$160	$1,296	$—	$1,456	$2,223
Operating margin	5.2 %	7.4 %	16.5 %	4.4 %	6.6 %	8.1 %
Adjusted operating margin (b)	5.4 %	7.5 %	23.4 %	4.4 %	7.2 %	8.6 %
Business disruption impacts - cyberattack (d)	$—	$—	$867	$—	$867	$867
Total cyberattack impacts	$494	$160	$2,163	$—	$2,323	$3,090

Takeaways for United Health?

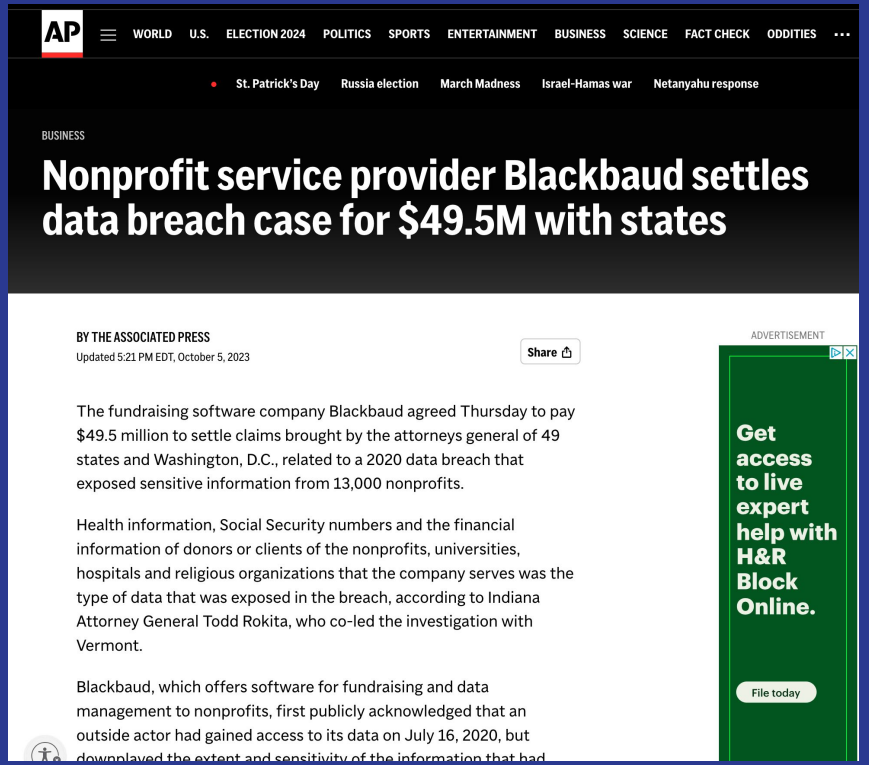
1. United Health is a prime example for investments in:
    - Data protection
    - Multi-factor authentication
    - Zero trust
    - Resilience
    - M&A due diligence services

2. **ASK:** Do we have money to self-insure?

3. **ASK:** What would the regulatory impact be?

Blackbaud

May 2020 Incident



AP

WORLD U.S. ELECTION 2024 POLITICS SPORTS ENTERTAINMENT BUSINESS SCIENCE FACT CHECK ODDITIES ...

St. Patrick's Day Russia election March Madness Israel-Hamas war Netanyahu response

BUSINESS

Nonprofit service provider Blackbaud settles data breach case for $49.5M with states

BY THE ASSOCIATED PRESS
Updated 5:21 PM EDT, October 5, 2023

Share

The fundraising software company Blackbaud agreed Thursday to pay $49.5 million to settle claims brought by the attorneys general of 49 states and Washington, D.C., related to a 2020 data breach that exposed sensitive information from 13,000 nonprofits.

Health information, Social Security numbers and the financial information of donors or clients of the nonprofits, universities, hospitals and religious organizations that the company serves was the type of data that was exposed in the breach, according to Indiana Attorney General Todd Rokita, who co-led the investigation with Vermont.

Blackbaud, which offers software for fundraising and data management to nonprofits, first publicly acknowledged that an outside actor had gained access to its data on July 16, 2020, but downplayed the extent and sensitivity of the information that had

What is Blackbaud?

- Creates software that helps nonprofits with Customer Relationship Management (CRM), marketing campaigns, fundraising, finance and accounting, and analytics.

- May 2020: Ransomware attack with over 100 customers affected, including at least twenty universities and charities based in the United Kingdom, the United States, the Netherlands and Canada

- Publicly traded on NASDAQ (BLKB)

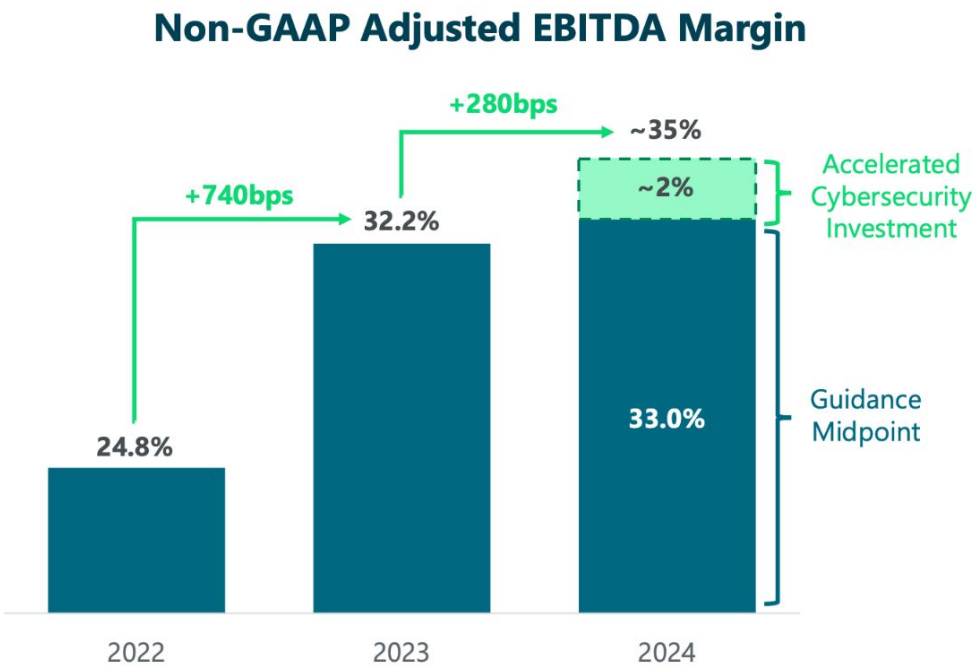

USD
Blackbaud, Inc. · 1D · NASDAQ
O54.73 H55.52 L51.44 C55.39 +0.11 (+0.21%)
71.34
0.17
71.51
SI ⌀ 1.376M
68.00
67.00
66.05
64.95
64.00
63.00
62.00
60.82
60.00
59.00
58.00
57.00
56.00
55.00
54.30
54.00
53.00
52.00
51.00
Jul 16:
Notified customers


HOLD ONTO YOUR BUTTS.

Strong non-GAAP adjusted EBITDA margin expansion

- Five-point operating plan drove 740 basis points of adjusted EBITDA margin expansion in 2023

- 2024 guidance is inclusive of a material, one-time step up in expense that will accelerate the completion of key security initiatives and will greatly benefit our customers for the long-term, including:
  - Cybersecurity talent (employees and third-party resources)
  - Systems and tooling to enhance identity & privilege access management and data loss prevention
- Absent this accelerated cybersecurity investment, 2024 adjusted EBITDA margins would have been ~200bps higher, or ~35%
- We do not expect the 2024 accelerated cybersecurity investment to repeat in 2025 and beyond



Significant management time and Company resources have been, and are expected to continue to be, devoted to the Security Incident. For example, for full year 2023, we incurred net pre-tax expenses of $53.4 million related to the Security Incident, which included $22.4 million for ongoing legal fees and $31.0 million for settlements and recorded liabilities for loss contingencies. During 2023, we had net cash outlays of $78.0 million related to the Security Incident, which included ongoing legal fees, the $3.0 million civil penalty paid during the first quarter of 2023 related to the SEC settlement and the $49.5 million civil penalty paid during the fourth quarter of 2023 related to the Multistate Investigation (as discussed in Note 11). Although we carry insurance against certain losses related to the Security Incident, we exceeded the limit of that insurance coverage in the first quarter of 2022. As a result, we will be responsible for all expenses or other losses (including penalties, fines or other judgments) or all types of claims that may arise in connection with the Security Incident, which could materially and adversely affect our liquidity and results of operations. (See Note 11 to our consolidated financial statements included in this report.) If

Expenses

- $22.4 million in ongoing legal fees
- $31.0 million for settlements + loss contingencies

$53.4 million total (2023)

Net Cash Outlays

- $3 million federal civil penalty
- $49.5 million state civil penalty
- Ongoing legal fees

$78.0 million in net cash outlays (2023)

What's the big deal?

Liquidity and Capital Resources

The following table presents selected financial information about our financial position:

(dollars in millions)	December 31, 2023
Cash and cash equivalents	$ 31.3
Property and equipment, net	98.7
Software and content development costs, net	160.2
Total carrying value of debt	779.7
Working capital	(267.4)

The following table presents selected financial information about our cash flows:

(dollars in millions)	2023
Net cash provided by operating activities	$ 199.6
Net cash used in investing activities	(64.4)
Net cash used in financing activities	(143.0)

40% of their cash was impacted by the attack.

How Much Did It Hurt (FY24)?

Security Incident update

As discussed in Note 11 to our consolidated financial statements included in this report, total costs related to the Security Incident exceeded the limit of our [redacted] Accordingly, the Security Incident has negatively impacted, and we expect it to continue for the foreseeable future to negatively impact, our GAAP profitability and GAAP cash flow (see discussion regarding non-GAAP free cash flow and non-GAAP adjusted free cash flow on page 53). For the year ended December 31, 2024, we incurred net pre-tax expenses of $13.7 million related to the Security Incident, which included $7.0 million for ongoing legal fees. It also includes settlements and recorded liabilities for loss contingencies of $6.8 million. Also, for the year ended December 31, 2024, we had net cash outlays of $15.9 million related to the Security Incident, which included ongoing legal fees and the $6.8 million paid during the third quarter of 2024 related to our settlement with the Attorney General of the State of California (as discussed in Note 11). In line with our policy, legal fees are expensed as incurred. For the year ended December 31, 2025, we currently expect net pre-tax expense of approximately $2.0 million to $3.0 million and net cash outlays of approximately $3.0 million to $4.0 million for ongoing legal fees related to the Security Incident.

[redacted] If any such fines or penalties were great enough that we could not pay them through funds generated from operating activities and/or cause a default under the 2024 Credit Facilities, we may be forced to renegotiate or obtain a waiver under the 2024 Credit Facilities and/or seek additional debt or equity financing. Such renegotiation or financing may not be available on acceptable terms, or at all. In these circumstances, if we were unable to obtain sufficient financing, we may not be able to meet our obligations as they come due.

Takeaways for Blackbaud?

1. Blackbaud is a prime example for investments in:
    - Encryption
    - Data protection
    - Cyber insurance

2. **ASK:** Would insurance cover your sensitive data loss impact? What percentage of the total loss?

3. Debt is king when you don’t have sufficient cash reserves.

National Public Data

2023 Breach


HOLD ONTO YOUR BUTTS.

What was National Public Data?

- A Florida-based background check firm. Not publicly traded.
- Leaked 2.9 billion records of PHI
- NPD’s parent company, Jerico Pictures, filed for Chapter 11 bankruptcy in Florida on October 2, 2023
- Full transcripts are restricted through June 3, 2025.

How Much Did It Hurt (FY24)?

In the wake of this overwhelming fallout, NPD's parent company, Jerico Pictures, filed for Chapter 11 bankruptcy in Florida on October 2. Court documents reveal that "the enterprise cannot generate sufficient revenue to address the extensive potential liabilities, let alone defend the lawsuits and support ongoing investigations."

Despite having gross revenues of over $1.15 million in 2023, the company lists assets of just over $44,000 and no physical offices, making it impossible to withstand the mounting legal pressures and financial demands triggered by the breach.

How Much Did It Hurt (FY24)?

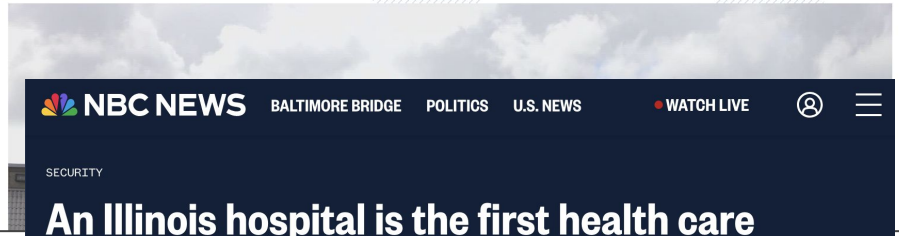
Background and Breach Incident

National Public Data came under scrutiny after an April 2024 data breach compromised approximately three billion records, including Social Security numbers and other personal information, affecting around 270 million individuals. Although much of the data was reportedly inaccurate, the breach ranked among the largest data incidents of 2024. Following the breach, National Public Data filed for bankruptcy protection, claiming it could not meet its financial obligations. However, the U.S. Bankruptcy Court for the Southern District of Florida dismissed the petition in November 2024, allowing creditors and regulatory bodies to proceed with legal action.

LOCAL NEWS

Florida-based radiology provider Akumin Imaging files for bankruptcy amid 'ransomware incident'

There are three Akumin Imaging centers in Jacksonville: Roosevelt Boulevard, Dunn Avenue, and Fort Caroline Road.

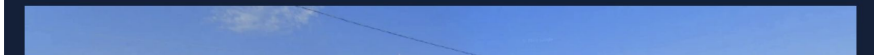


NBC NEWS BALTIMORE BRIDGE POLITICS U.S. NEWS WATCH LIVE

SECURITY

An Illinois hospital is the first health care facility to link its closing to a ransomware attack

A ransomware attack hit SMP Health in 2021 and halted the hospital's ability to submit claims to insurers, Medicare or Medicaid for months, sending it into a financial spiral.



NEWS 10 AUG 2020

Travelex Forced into Administration After Ransomware Attack

Phil Muncaster
UK / EMEA News Reporter, Infosecurity Magazine
Email Phil Follow @philmuncaster

Ransomware victim Travelex has been forced into administration, with over 1000 jobs set to

THE HIPAA JOURNAL

The HIPAA Journal is th
and indepe

Become HIPAA Compliant » HIPAA News » HIPAA Compliance Checklist Latest HIPAA Updates » HIPAA Training » About Us »

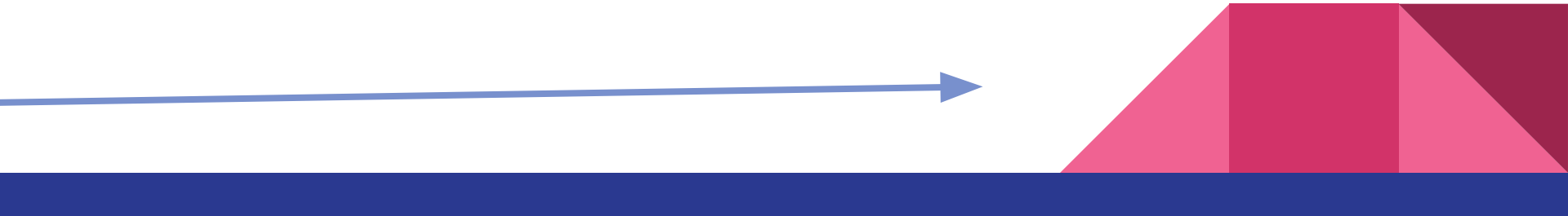
Petersen Health Care Files for Bankruptcy Following Ransomware Attacks

Posted By Steve Alder on Mar 22, 2024

Peoria, Illinois-based Petersen Health Care, one of the largest operators of nursing homes in the United States, filed for Chapter 11 protection in a Delaware bankruptcy court on Wednesday following cyberattacks that led to defaults on government-backed loans. Petersen Health Care operates more than 90 nursing homes in Illinois, Missouri, and Iowa, employs almost 4,000 people, and has almost 6,800 residents. The company had more than $339 million in revenue in 2023 but has debts of more than $295 million, including $45 million owed on healthcare facility

Takeaways for NPD?

1. NPD is a prime example for investments in:
    - Encryption
    - Data protection
2. **ASK:** How much cash do we have on-hand?
3. **<u>Bankruptcy will not save you!</u>**



Stoli

2024 August Cyber Attack

Stoli vodka owners file for bankruptcy following cyberattack

The company's CEO said that its IT systems have been affected since the ransomware attack earlier this year, which coincided with the seizure of distilleries producing the spirit in Russia.

Published Dec. 4, 2024

Chris Casey
Staff Reporter

What is Stoli?

- An American subsidiaries of Stoli Group. The vodka brand, which was first sold in the U.S. in the 1970s. In 2022, the company changed its name from Stolichnaya to Stoli following the Russian invasion of Ukraine

- The Russian government labeled the Stoli Group as “extremists” and seized the brand’s two remaining distilleries within the country last summer

- Stoli experienced a ransomware attack in August

Takeaways for Stoli?

1. Stoli is a prime example for investments in:
    - Business continuity & disaster recovery
    - Cyber insurance

2. **ASK:** Is there a nation-state that we might anger with our values or political beliefs? How do we insulate ourselves?

3. **<u>Geopolitical impacts are REAL.</u>**

Clorox

2023 Cyber Attack

Alessandro Mascellino
Freelance Journalist
Email Alessandro Follow @a_mascellino

Cleaning product manufacturer Clorox has confirmed significant operational disruption caused by a recent cyber-attack.

According to a notice published on the company's website, the attack was detected on August 14, prompting Clorox's IT team to take immediate action by halting suspicious activity and shutting down affected systems. As a precautionary measure, the

What is Clorox?

- They are an American global manufacturer and marketer of consumer and professional products such as Clorox bleach, Burt's Bees, Glad, Hidden Valley, Kingsford, KC Masterpiece, Liquid-Plumr, Brita, Pine-Sol, and Scoop Away.

- Aug 2023: Notification to SEC of unauthorized activity. “The incident has caused, and is expected to continue to cause, disruption to parts of the Company’s business operations”

- Publicly traded on NYSE (CLX)


USD
Clorox Company (The) · 1D · NYSE
O157.63 H158.72 L156.78 C157.06 −0.03 (−0.02%)
152.23
0.07
152.30
SI ⌀ 862.382K
168.00
164.00
160.00
156.00
152.29
02:29:01
148.00
146.09
144.00
140.94
139.17
136.00
132.00
128.00
124.00
120.00
116.00
112.00
Aug 11:
Incident started
on Friday.
Aug 14:
SEC notification
of incident by Monday.
Sep 18:
SEC filing of
material impact.
Note the increase
in short seller activity
before the filing.
Note the increase
in shorts betting the
stock would tank further.
E
D
D
E

NOTE 2. CYBERATTACK

On Monday, August 14, 2023, the Company disclosed it had identified unauthorized activity on some of its Information Technology (IT) systems. That activity began on Friday, August 11, 2023 and after becoming aware of it that evening, the Company immediately began taking steps to stop and remediate the activity. The Company also took certain systems offline and engaged third-party cybersecurity experts to support its investigation and recovery efforts. The Company implemented its business continuity plans, including manual ordering and processing procedures at a reduced rate of operations in order to continue servicing its customers. However, the incident resulted in wide-scale disruptions to the Company's business operations throughout the remainder of the quarter ended September 30, 2023.

The impacts of these system disruptions included order processing delays and significant product outages, resulting in a negative impact on net sales and earnings. The Company has since transitioned back to automated order processing. The Company experienced lessening operational impacts in the second quarter as it made progress in returning to normalized operations.

Six Months Ended

- $20 million costs of products sold
- $29 selling and administrative expenses

$49 million in expenses

of the cyberattack for the three and six months ended December 31,
d consolidated statements of earnings and comprehensive income:

Three months ended	Six months ended
12/31/2023	12/31/2023
$ 9	$ 20
16	29
$ 25	$ 49

and forensic experts and other professional services incurred to
e resulting disruption to the Company's business operations. The
Company has not recognized any insurance proceeds in the three and
insurance recoveries, if any, may differ from the timing of

Bloomberg

Technology | Cybersecurity

Clorox Audit Flagged Systemic Flaws in Cybersecurity at Manufacturing Plants

An internal review in 2019 and 2020 found that production systems weren't properly protected by firewalls and security appliances, three former employees said. Clorox says the findings weren't relevant to an August 2023 breach.

The hack cost Clorox about $350 million in sales declines, and it is expected to incur costs of up to $109 million related to the hack itself, according to Mills. Clorox's sales rose in the latest quarter as it rebuilt store inventories across the country. The company said in February that it had recovered 86% of the distribution that it lost due to the breach. It still hasn't fully restocked shelves for certain categories like cat litter and Glad bags, Chief Financial Officer Kevin Jacobsen said in a February interview.

The vulnerabilities identified by the audit didn't play a role in how the hackers got into Clorox's systems, according to the company.

$350 million in sales declines **$109 million costs**

What’s the big deal?

Capital Resources and Liquidity

The Company's current liabilities may periodically exceed current assets as a result of the Company's debt management policies, including the Company's use of commercial paper borrowings which fluctuates depending on the amount and timing of operating and investing cash flows and payments for shareholder transactions such as dividends. The Company continues to take actions to address some of the effects of such cost increases, which include implementing price increases, driving cost savings and optimizing the Company’s supply chain.

Notwithstanding potential unforeseen adverse market conditions and as part of the Company’s regular assessment of its cash needs, the Company believes it will have the funds necessary to support its short- and long-term liquidity and operating needs, including the costs related to the announced streamlined operating model and its digital capabilities and productivity enhancements investment, as well as the costs and impacts of the business disruption associated with the cyberattack, based on our anticipated ability to generate positive cash flows from operations in the future, access to capital markets enabled by our strong short-term and long-term credit ratings and current borrowing availability.

The Company believes it will have the funds necessary to support [..] its operating needs, including [..] the costs and impacts of the business disruption associated with the cyberattack, based on our anticipated ability to **generate positive cash flows from operations in the future**, **access to capital markets** enabled by our strong short-term and long-term credit ratings and current borrowing availability.

What's the latest (FY24)?

- **YES:** "Net sales decreased 15% to $1.69 billion compared to a 16% net sales increase in the year-ago quarter.

- **BUT:** "A 21 cent benefit to earnings per share from cyberattack insurance recoveries in the first half of this fiscal year"

- **AND CEO Linda Rendle said:** "If you look at the growth in the cleaning business, it's like the cyberattack never happened."

How Much Did It Hurt (FY24)?

NOTE 4. AUGUST 2023 CYBERATTACK

On Monday, August 14, 2023, the Company identified unauthorized activity on some of its Information Technology (IT) systems and immediately began taking steps to stop and remediate the activity. The Company took certain systems offline, engaged third-party cybersecurity experts and implemented its business [redacted] the incident resulted in wide-scale disruptions to the Company's business operations. The impacts of these system disruptions resulted in a negative impact on net sales and earnings. The Company experienced lessening operational impacts in the second quarter of fiscal year 2024 and has since returned to normalized operations.

The costs incurred related primarily to third-party consulting services, including IT recovery and forensic experts and other professional services incurred to investigate and remediate the attack, as well as incremental operating costs incurred from the resulting disruption to the Company's business operations. The Company does not expect to incur significant costs related to the cyberattack in future periods. No additional insurance recoveries related to the cyberattack are anticipated. Insurance recoveries are classified consistent with the expenses to which they relate. Business interruption and other insurance recoveries that do not correspond directly to previously incurred expenses are recognized in Other (income) expense, net.

Takeaways for Clorox?

1. Clorox is a prime example for investments in:
    - Resilience
    - Cyber insurance

2. **ASK:** How much cyber insurance do we carry?

3. **ASK:** Do we care about cyber if manufacturing is isolated and we have no sensitive data?

4. **<u>No sensitive data leakage = no problem?</u>**

What should we do with this info?

"CISOs [and cybersecurity sales professionals] need to translate the cybersecurity request for funds into the language of the rest of the organization"

— Jay paraphrasing Doug Hubbard

Tell Better Stories

Know your organization; know your customer. Context matters.

REMINDER:

“The human mind is a story processor, not a logic processor.”

— Jonathan Haidt

Takeaways

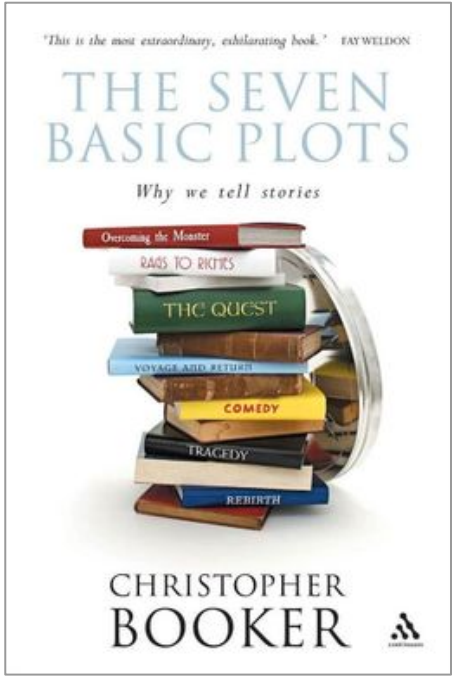
1. Understand the emotion behind the need; connect personally and develop meaningful relationships

2. Use financial impact to tell meaningful cybersecurity stories that aid your champions/buyers/stakeholders with communicating the request for funds

    - Protagonist
    - A Great Mistake
    - Rebirth or Tragedy

Resources

- SEC: “How To Read a 10K/10Q”
  - https://www.sec.gov/oiea/investor-alerts-and-bulletins/how-read-10-k10-q
  - https://www.sec.gov/files/reada10k.pdf
- Warren Buffett: How To Analyze Financial Statements
  - https://www.youtube.com/watch?v=H9pmFe1vpu8
- How To Analyze a Cash Flow Statement
  - https://www.youtube.com/watch?v=1v8hRZ36--c
- Corporate Debt Securities in US Capital Markets
  - https://www.lexisnexis.com/community/insights/legal/practical-guidance-journal/b/pa/posts/corporate-debt-securities-in-u-s-capital-markets
- *The Seven Basic Plots* by Christopher Booker



Fin.

Want to connect?
Find me on LinkedIn.