~~10~~ Things I Hate About Application Security

Best practices + anti-patterns

For OWASP Columbus

10

The proliferation of API security tools: agent & agent-less

API security is legit?

What do we really need to solve?

- Where is the gap really? Where do we need VC-backed startups to sell us an enterprise tool.
- **DO have an API inventory**
- **DO have an inventory of your controllers, actions and endpoints**

9

Worrying about supply chain security

SBOMs & supply chain

The community approach works

- We don’t need another tool for this. We need advocacy and financial incentives.
- **DO use SBOMs to improve your vuln management**
- **DO compensate maintainers**

8

Fake security champion programs and poor training

Real recognize real

Provide feedback and power

- Capture the flag events and “think like a hacker” chat.
- **DO democratize security by giving champions power**
- **DO tighten the feedback loop and share findings widely as a part of training**

jaybobo

7

Poor tooling: CodeQL, snyk, dependabot, veracode, etc

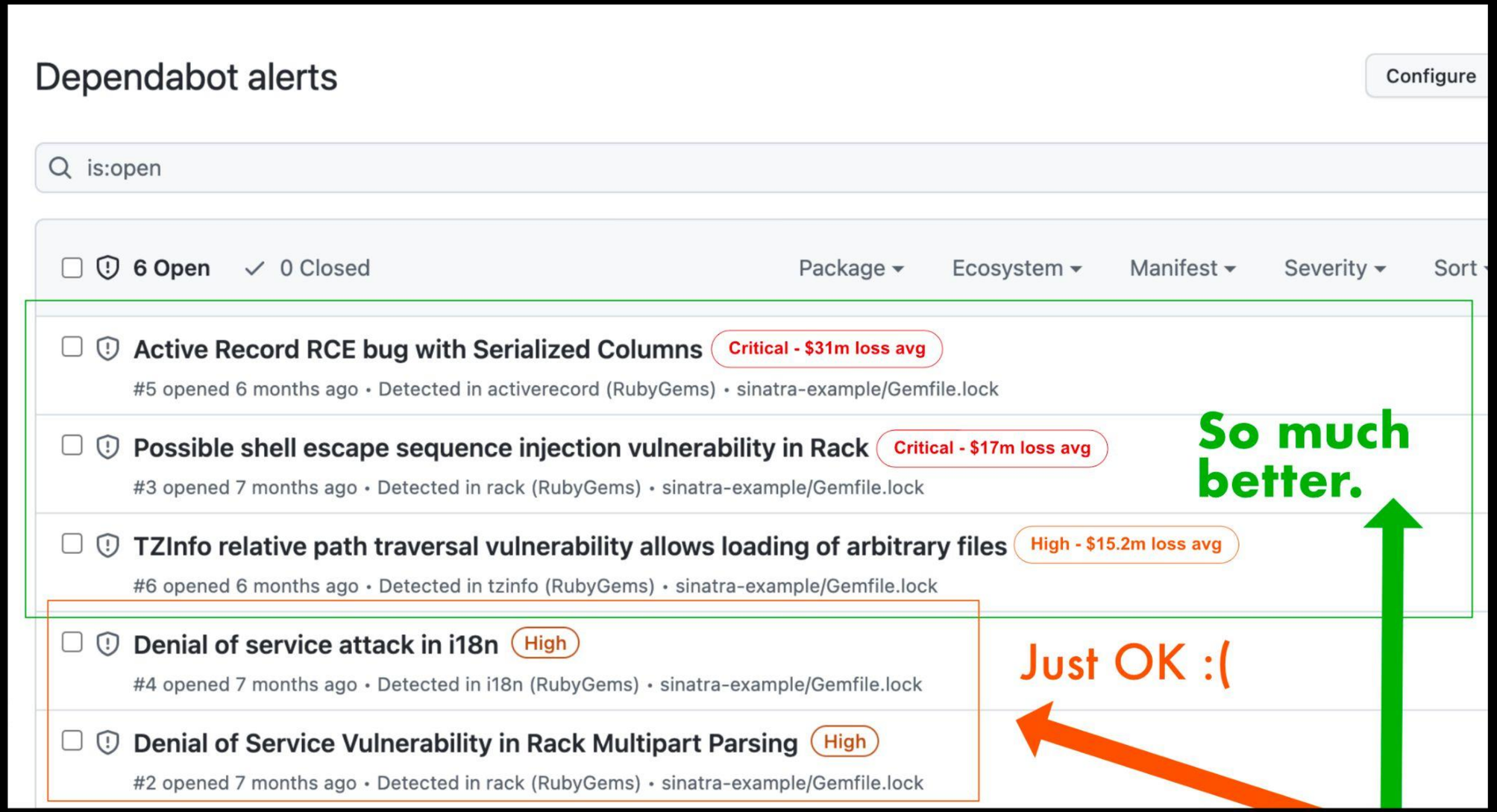
Is this a real finding?

More noise, less signal.

- They often create more work. When will a vendor use a truly risk based approach?
- **DO have a process for quickly assessing business-critical risk**

jaybobo

Deep Dive:



Make security tools better with loss data

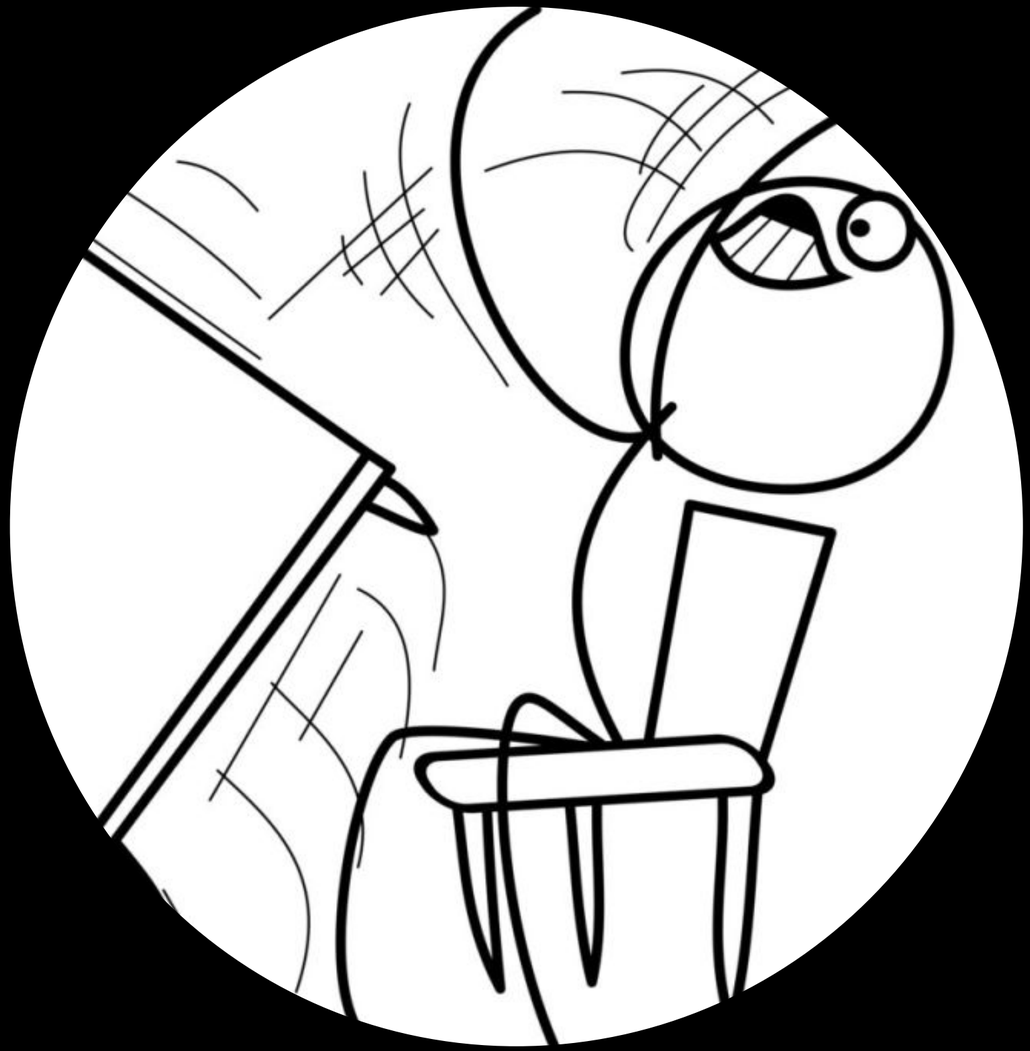
6

Not having a process for business logic issues.

Poor relationships

See something, say something?

- AppSec teams are expensive and don’t scale well across a broad organization.
- **How do you catch the stuff that SAST and SCA scans can’t see?**



5

The lack of focus on vuln management.

Why remediate?

What does the data say?

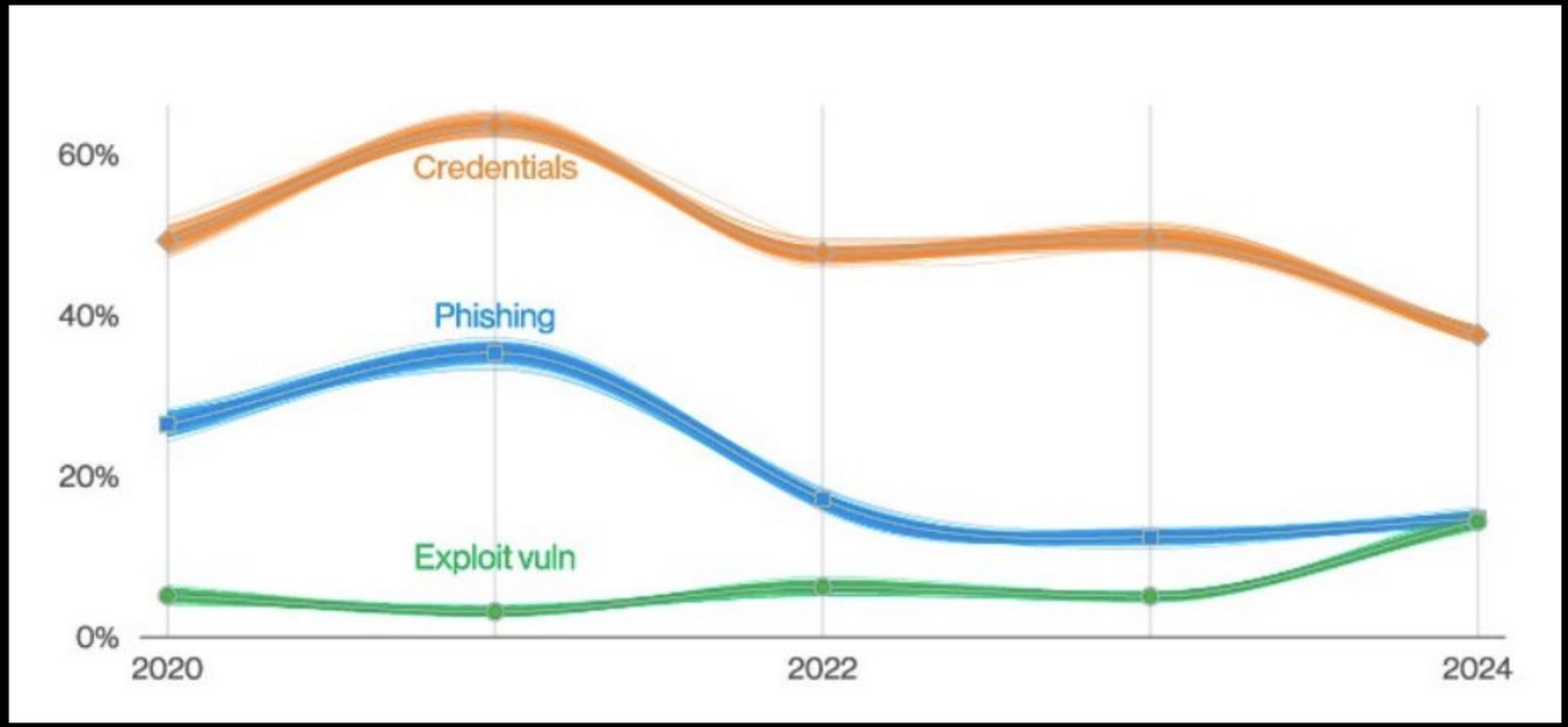
- The most important part of your program isn’t application security but vulnerability remediation.
- **Are you not focused on remediation? Why not?**

Deep Dive:

Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

jaybobo

Deep Dive:



4

Using the same pentesters and methodology every year.

Does it matter?

Blackbox, greybox, whitebox

- If your pentest vendors are the same every year, then expect diminishing returns.
- **If you’re focused on compliance, does it matter?**

3 No risk component

3a

“We don’t have enough data to do security right!”

Blackjack & AppSec

It’s all in the data

- We have enough information to know our focus should be phishing and vulnerability management.
- **Are there systems for making good decisions without complete information?**

3b

“Reputational damage can’t be measured”

Reputational damage

Maybe awesome, maybe not!

- Susie’s competitor, Little Johnny tells the whole neighborhood that Susie puts rat poison in her lemonade.
- **How would we measure reputational damage to Susie?**

2

Lacking data to tell security stories that matter

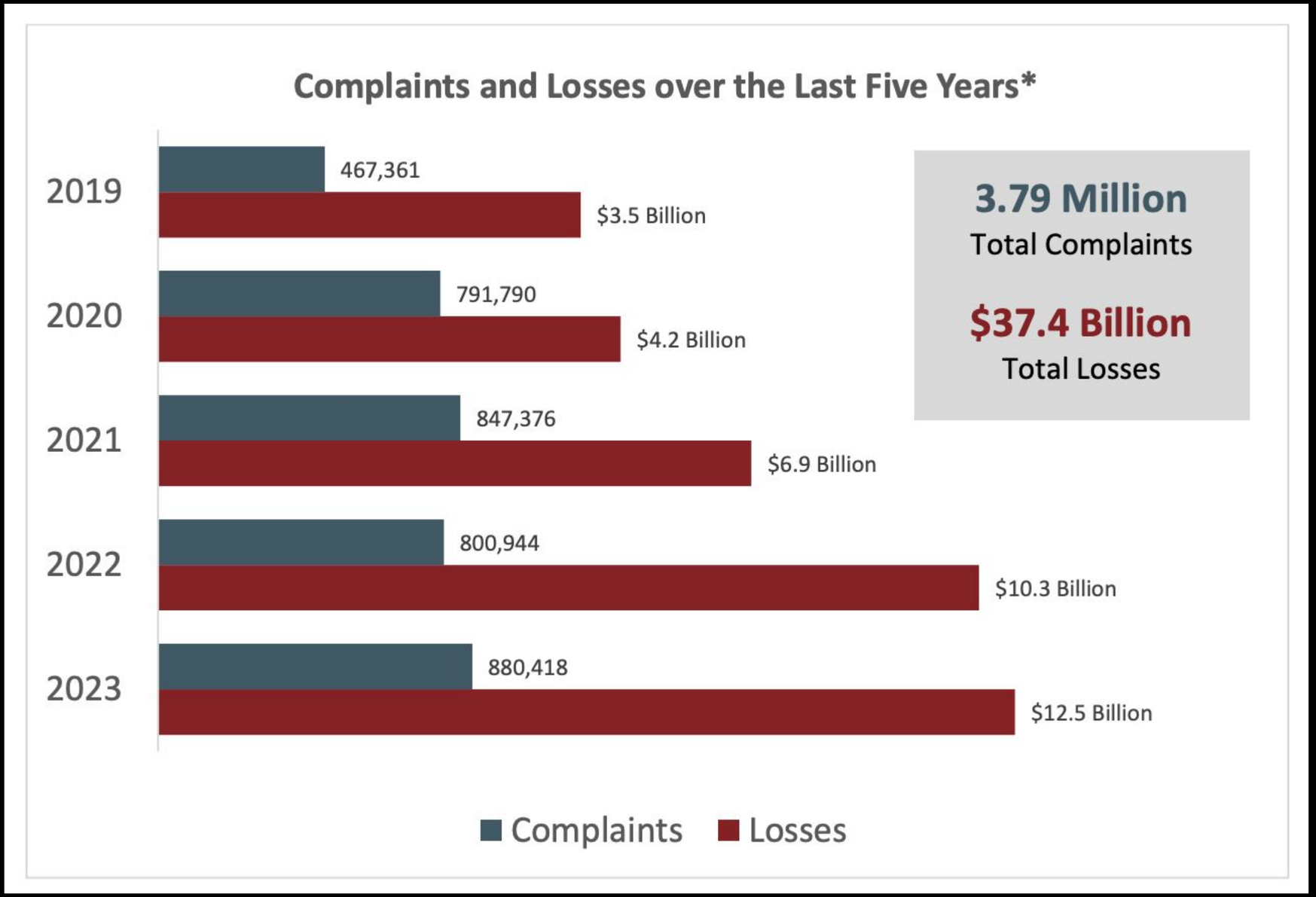
breachsiren

An additional factor that makes assessing such risk difficult for the CEO is a suspicion that the cybersecurity team and/or professional advisers can exaggerate the risk of an attack in order to extract more budget or consultancy hours.

Source: The 2023 CEO Report on Cyber Resilience, Istari + Oxford University

Problem: Trust

Deep Dive:


Complaints and Losses over the Last Five Years*
2019
467,361
$3.5 Billion
2020
791,790
$4.2 Billion
2021
847,376
$6.9 Billion
2022
800,944
$10.3 Billion
2023
880,418
$12.5 Billion
3.79 Million
Total Complaints
$37.4 Billion
Total Losses
Complaints
Losses

Deep Dive:

2023 CRIME TYPES

By Complaint Count			
Crime Type	*Complaints*	*Crime Type*	*Complaints*
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		
*Descriptors**			
Cryptocurrency	43,653	Cryptocurrency Wallet	25,815

jaybobo

Deep Dive:

2023 CRIME TYPES continued

By Complaint Loss			
Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		
*Descriptors***			
Cryptocurrency	$3,809,090,856	Cryptocurrency Wallet	$1,778,399,729

1

Focusing on the tech and forgetting the big picture

What matters most?

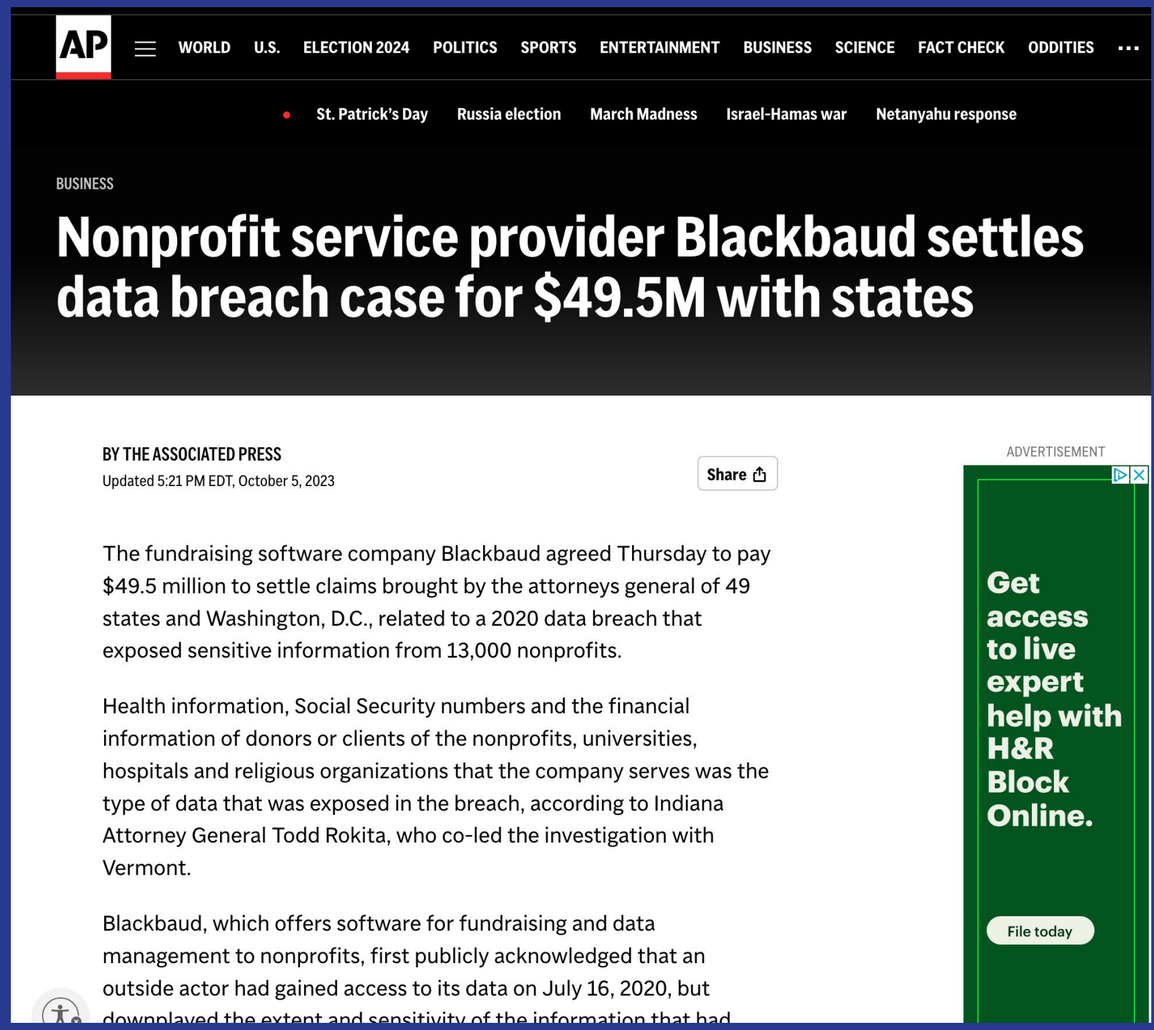
Alice in AppSec Wonderland

- Engineers and managerswill often disappear down the optimization and security blackhole.
- **Enabling the business is important? Why?**

Story Time

Blackbaud

A story of woe



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)


HOLD ONTO YOUR BUTTS.

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 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 2020 Credit Facility, we may be forced to renegotiate or obtain a waiver under the 2020 Credit Facility 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.

Expenses

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

$53.4 million total

Net Cash Outlays

- $3 million federal civil penalty
- $49.5 million state civil penalty

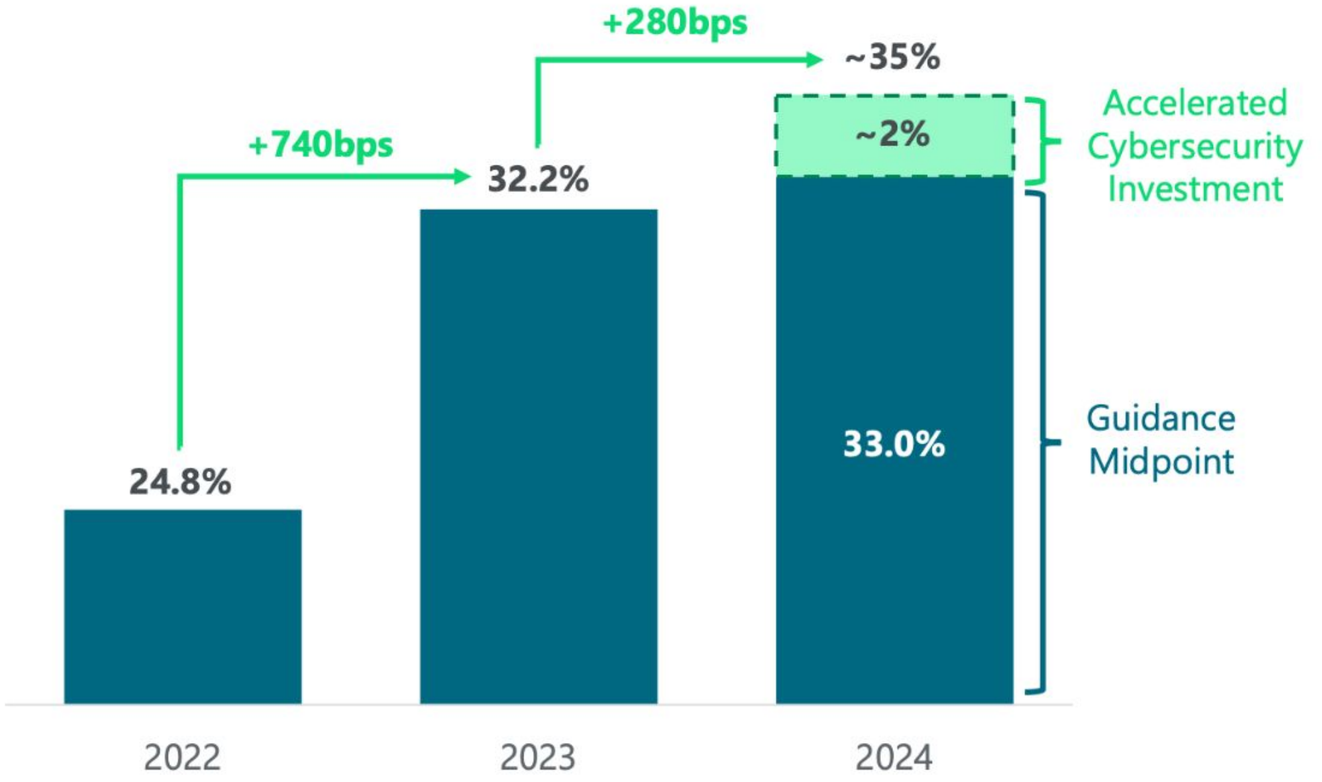
$78.0 million in net cash outlays

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

Non-GAAP Adjusted EBITDA Margin



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.

Clorox

What’s the difference?

NEWS 16 AUG 2023

Clorox Operations Disrupted By 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

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**

Small business?

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.

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

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.

THE HIPAA JOURNAL

The HIPAA Journal is
and inde

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

Petersen Health Care Files for Bankruptcy Following Ransomware Attacks

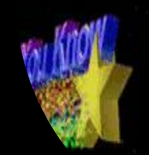
Posted By Steve Alder on Mar 22, 2024

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

I’m Done.

Any questions?

Recommendations…



- For cyber loss data:
  - Verisk, IHS Markit, Zywave, breachsiren.com
- For breach notification data:
  - Vcdb, breachsiren.com
- Risk quantification:
  - “How to Measure Anything in Cybersecurity Risk” by Doug Hubbard
  - *FAIR Blog: Shopping for Cyber Loss Data* by Allison Seidel