DM ENTERPRISE GROUP Presents...

RANSOMWARE... NOT ON MY WATCH!

Sponsored By:

THRIVE℠

IN BUSINESS FOR 23 YEARS WITH LESS THAN 1% CLIENT ATTRITION

600+

Active Clients

- Financial Services
- Healthcare
- Public Sector/Education
- Retail
- Manufacturing/Industrial Services
- Other

>1,500

Projects Delivered

- Telephony
- Network
- UCaaS
- CCaaS
- Managed Services
- Wireless
- Artificial Intelligence
- Cybersecurity
- IaaS
- Variable Labor

>$350mm

Returned

- Lower-cost alternative solutions
- Business optimization
- Revenue generating
- Credits returned
- New market solutions
- Solution consolidation

ACTIVITY CONTINUES TO RISE

"However, successful ransomware attacks are growing faster. **Publicly disclosed attacks surged by 96% in the first four months of 2024**, compared to the same period in 2023, continuing a worrying trend after a 68% increase the previous year. High-profile victims so far this year include Claro, First American, Hyundai, Norsk Hydro and Subway. This trend is unsustainable."

– Jay McBain, Canalys

https://www.linkedin.com/pulse/total-cybersecurity-spending-reach-250-billion-2024-partner-mcbain-leqye/

DM
ENTERPRISE GROUP

ACTIVITY CONTINUES TO RISE

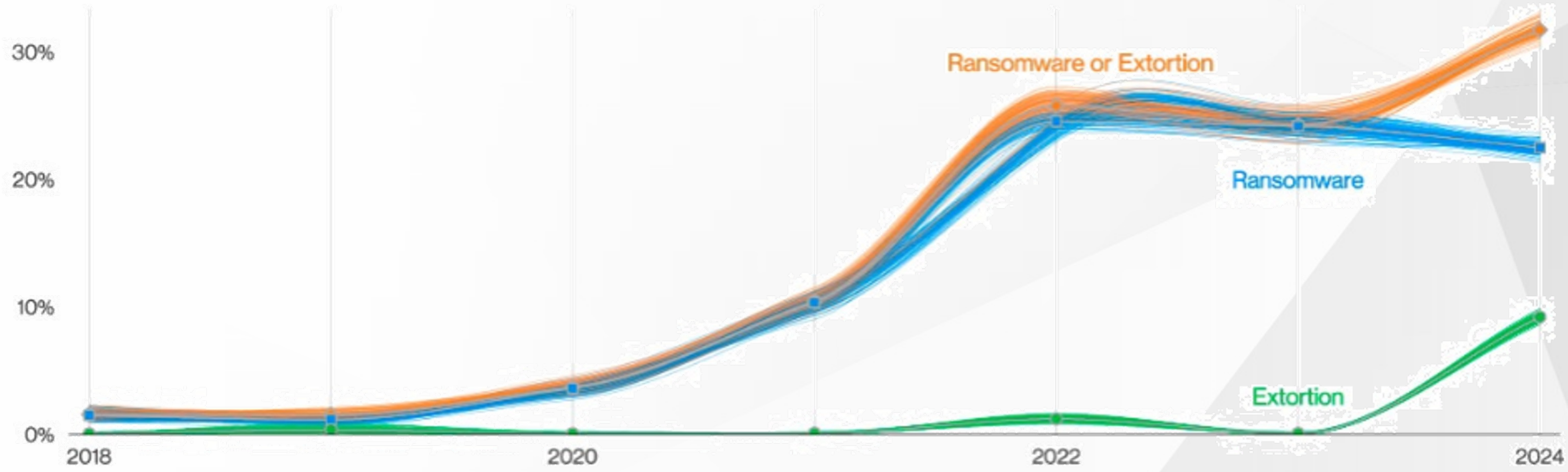
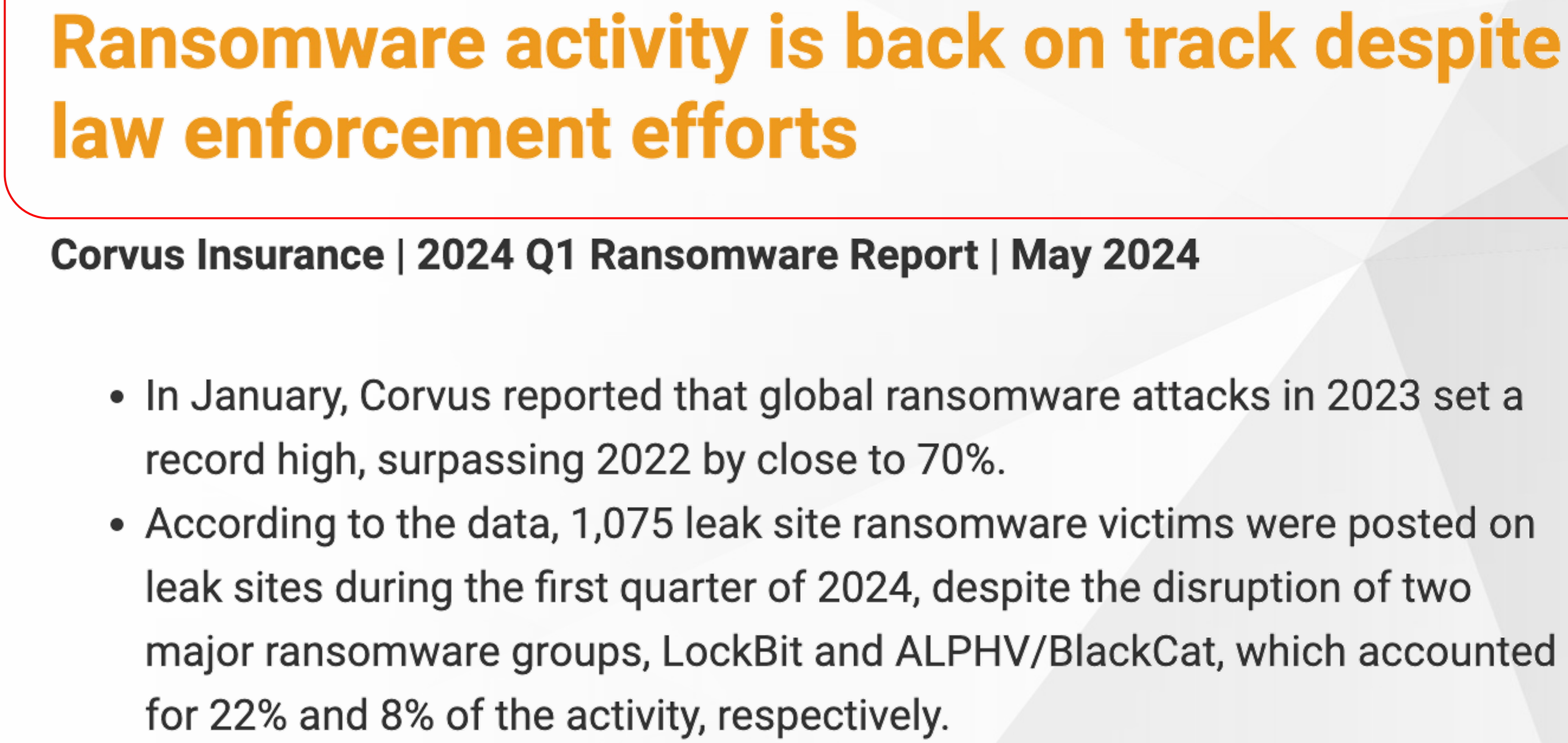


Figure 2. Ransomware and Extortion breaches over time

"Verizon 2024 Data Breach Investigations Report"

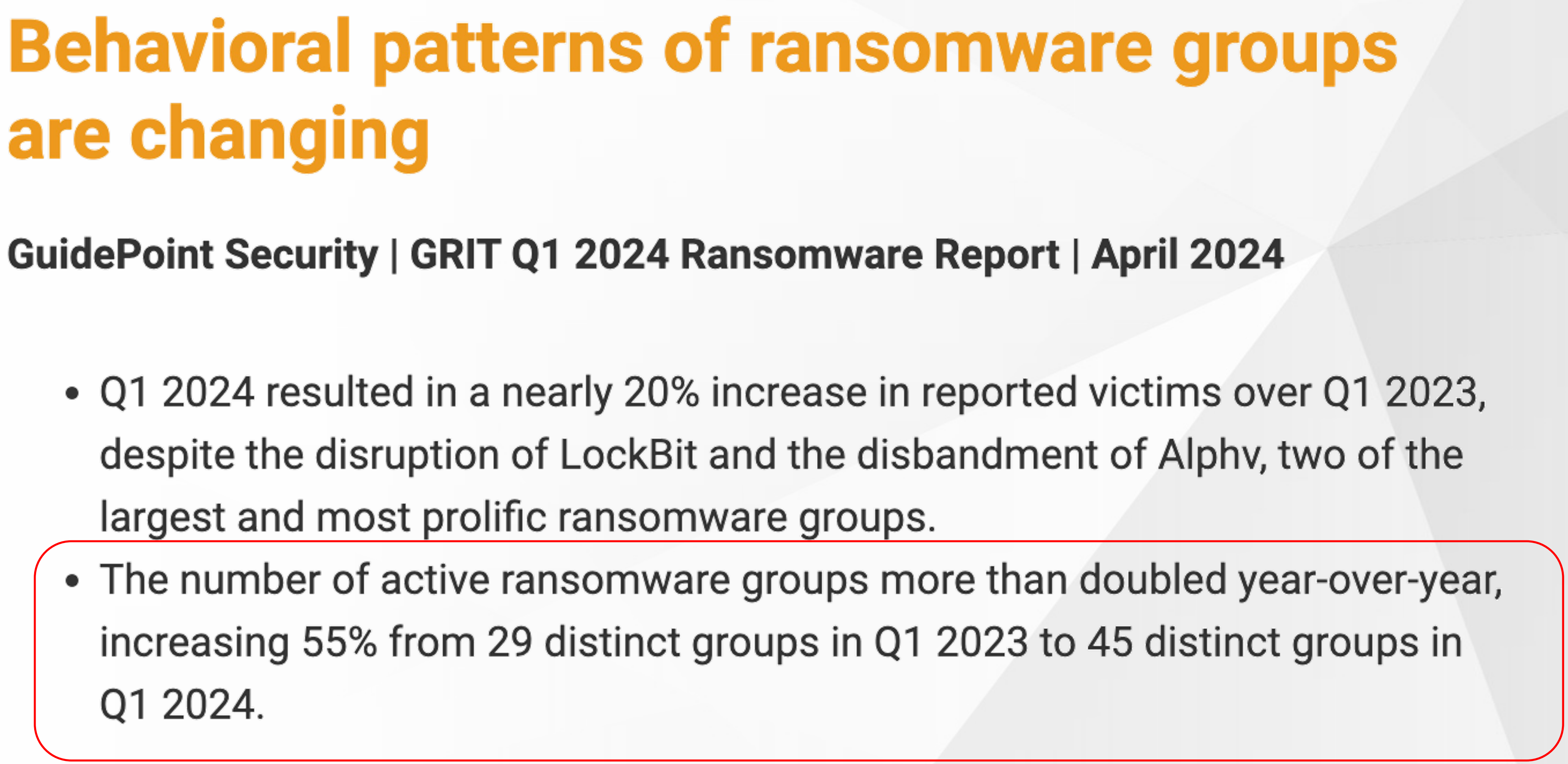


Ransomware activity is back on track despite law enforcement efforts

Corvus Insurance | 2024 Q1 Ransomware Report | May 2024

- In January, Corvus reported that global ransomware attacks in 2023 set a record high, surpassing 2022 by close to 70%.
- According to the data, 1,075 leak site ransomware victims were posted on leak sites during the first quarter of 2024, despite the disruption of two major ransomware groups, LockBit and ALPHV/BlackCat, which accounted for 22% and 8% of the activity, respectively.

https://www.helpnetsecurity.com/2024/05/15/ransomware-statistics-2024/

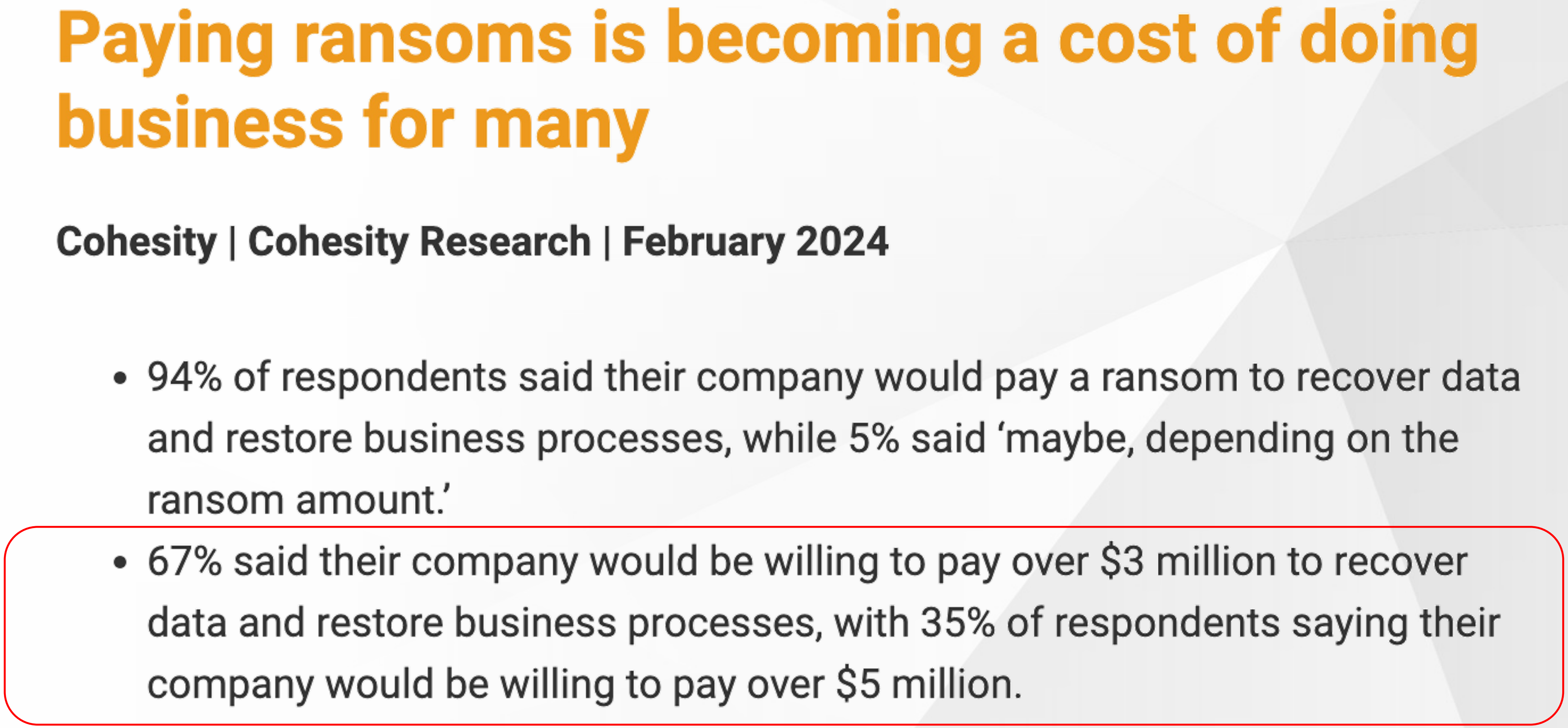


Behavioral patterns of ransomware groups are changing

GuidePoint Security | GRIT Q1 2024 Ransomware Report | April 2024

- Q1 2024 resulted in a nearly 20% increase in reported victims over Q1 2023, despite the disruption of LockBit and the disbandment of Alphv, two of the largest and most prolific ransomware groups.
- The number of active ransomware groups more than doubled year-over-year, increasing 55% from 29 distinct groups in Q1 2023 to 45 distinct groups in Q1 2024.

https://www.helpnetsecurity.com/2024/05/15/ransomware-statistics-2024/

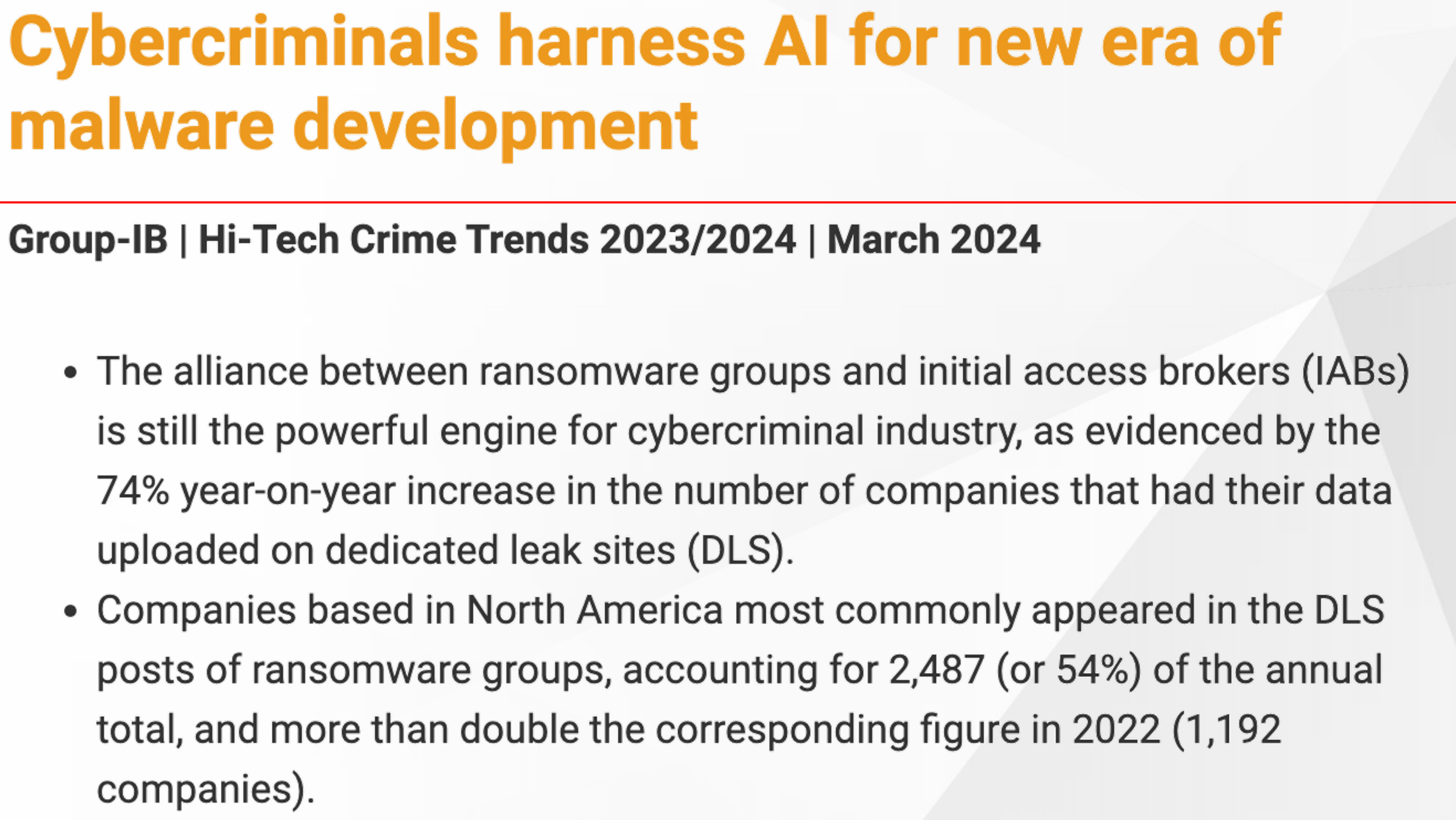


Paying ransoms is becoming a cost of doing business for many

Cohesity | Cohesity Research | February 2024

- 94% of respondents said their company would pay a ransom to recover data and restore business processes, while 5% said 'maybe, depending on the ransom amount.'
- 67% said their company would be willing to pay over $3 million to recover data and restore business processes, with 35% of respondents saying their company would be willing to pay over $5 million.

https://www.helpnetsecurity.com/2024/05/15/ransomware-statistics-2024/



Cybercriminals harness AI for new era of malware development

Group-IB | Hi-Tech Crime Trends 2023/2024 | March 2024

- The alliance between ransomware groups and initial access brokers (IABs) is still the powerful engine for cybercriminal industry, as evidenced by the 74% year-on-year increase in the number of companies that had their data uploaded on dedicated leak sites (DLS).
- Companies based in North America most commonly appeared in the DLS posts of ransomware groups, accounting for 2,487 (or 54%) of the annual total, and more than double the corresponding figure in 2022 (1,192 companies).

https://www.helpnetsecurity.com/2024/05/15/ransomware-statistics-2024/

WHO'S JOB IS AT RISK?

□ **Chief Information Security Officer (CISO):** The CISO is primarily responsible for the security of the company's information and data. If a significant breach occurs, the CISO might be held accountable for failing to protect the company.

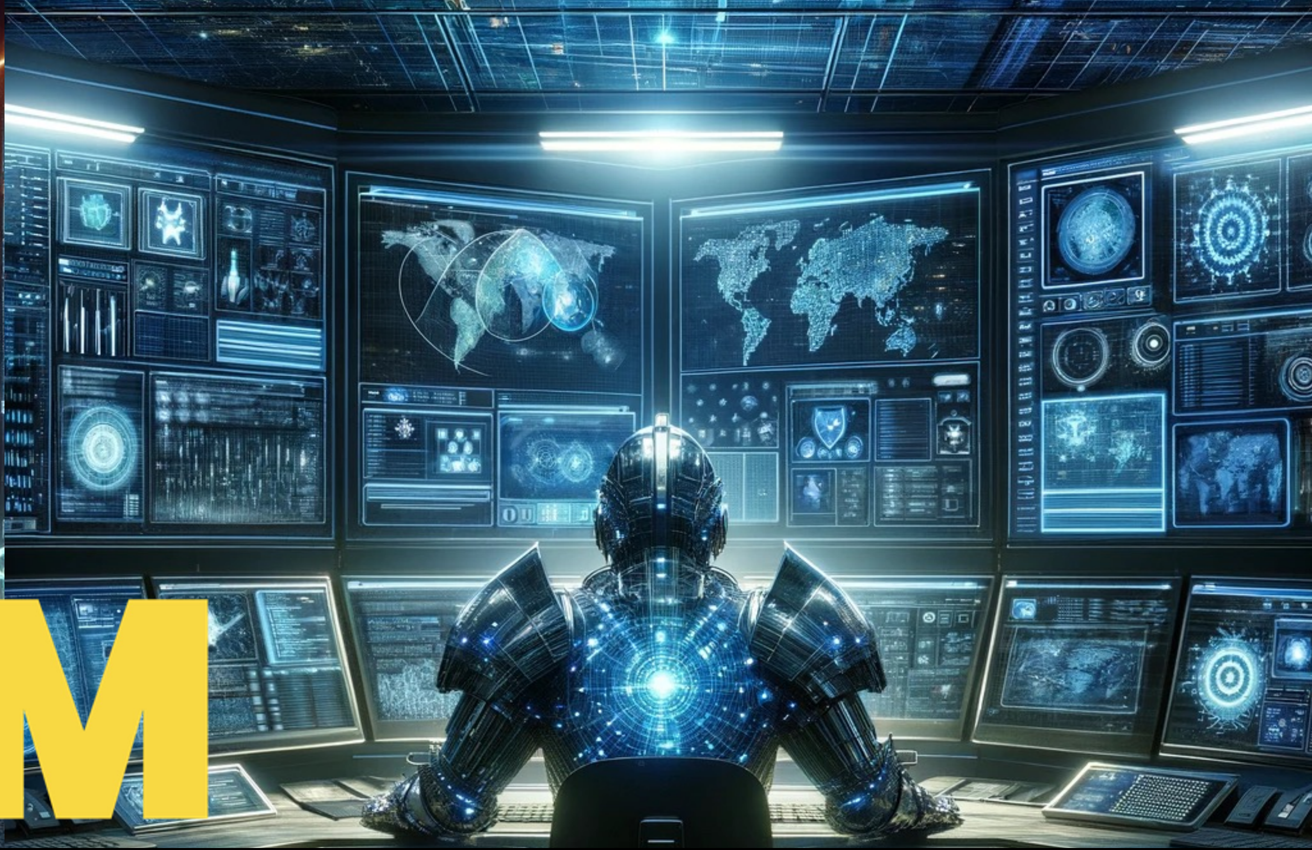
□ **IT Security Team Members:** Depending on the severity of the breach and internal investigations, members of the IT security team might be let go if they are found to have neglected their duties or failed to follow proper protocols.

□ **Chief Information Officer (CIO):** The CIO oversees the entire IT department, including security. In some cases, the CIO might also be held accountable for the breach, especially if there were known vulnerabilities that were not addressed.

□ **IT Department Staff:** Broader layoffs within the IT department could occur, particularly if systemic issues are identified or if the company decides to restructure its IT operations in response to the attack.

□ **Third-Party Contractors:** If the breach is linked to the negligence or failure of third-party contractors or vendors, those contracts may be terminated, and individuals working for those third parties could lose their jobs.

□ **Executive Management:** In extreme cases, other members of the executive team might face scrutiny, especially if the breach leads to significant financial loss, regulatory penalties, or damage to the company's reputation.



DM

ENTERPRISE GROUP

88 West Front Street
Keyport, NJ 07735

888-357-5055 – Office

www.dmenterprise.net

info@dmenterprise.net

www.dmenterprise.net