adlumin

Protecting SMBs: Key Cybersecurity Data Insights

Adlumin brings you a comprehensive visual overview of key statistics and trends. Shedding light on the evolving landscape of cybersecurity threats and challenges small and medium-sized businesses (SMBs) face.

Top Industries Targeted

Higher Education:
Higher ed is a prime target for cybercriminals due to the wealth of student and employee personal data, lack of security awareness and lagging cybersecurity processes and measures.

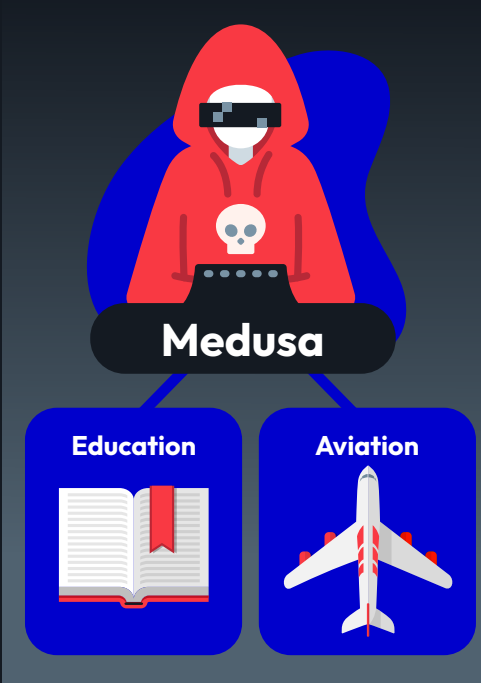
BioTechnology:
Biotech organizations hold access to personal data and medical records. This wealth of data lures cybercriminals in and creates potential risks for these organizations.

Government:
Cybercriminals target government administration organizations looking to resell stolen consumer data and cause expensive data breaches.

Top Tactic Used: Double Extortion

Threat Landscape

Groups with most victims + targeted industries



20% Adlumin recorded a 20% surge in security threat detections, reflecting a rise in cyberattacks on customer infrastructure.

30% Security Orchestration and Automated Response (SOAR) capabilities were used to combat rising threats, leading to a 30% increase in automated remediation actions.

Popular Vulnerabilities Found in the Wild

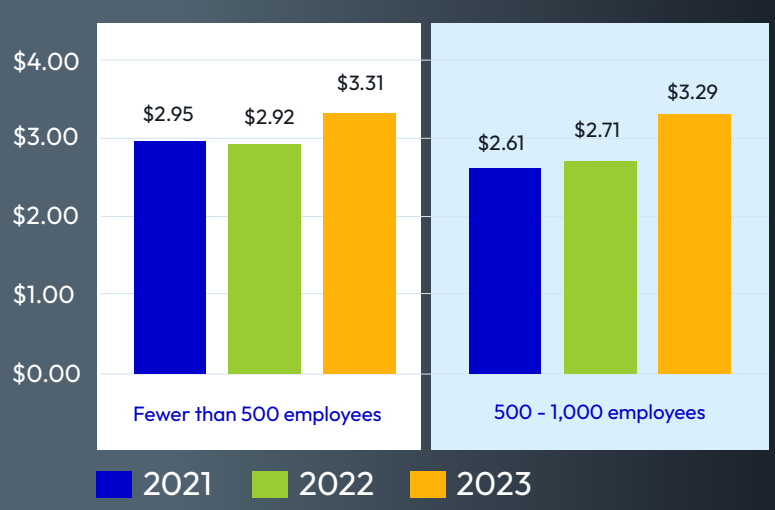
2,373
Average monthly vulnerabilities

With CVEs rising daily, organizations must stay proactive in securing their enterprise networks through patch management. Patching and remediation are key to reducing the vulnerabilities operations team must chase down as part of a remediation cycle.

Cost of Data Breaches for SMBs

Businesses with 500–1,000 employees increased by 21.4%, while companies with 1,001– 5,000 employees increased by nearly 20%.

$3.5M



Proactive Cybersecurity Awareness

Security awareness training is essential for educating individuals on potential security risks and teaching them how to protect themselves, organizations, and their sensitive information.

Proactive Cybersecurity Awareness Programs:

Empower Employees

Strengthen Defenses

Bring Awareness to Cyber Risks

91% of successful data breaches started with a spear phishing attack

81.5% After 90 days of completing monthly or more frequent security training, the likelihood an employee will click a phishing email decreases to 18.5%

Learn more at adlumin.com

References:

[1] https://www.ibm.com/downloads/cas/E3G5JMBP

[2]https://3431514.fs1.hubspotusercontent-na1.net/hubfs/3431514/2022%20Marketing%20Collateral/Reports/COM-0079-Threat%20Report.pdf

[3]https://3431514.fs1.hubspotusercontent-na1.net/hubfs/3431514/2022%20Marketing%20Collateral/Reports/COM-0091-Adlumin%E2%80%99s%20Cyber%20Threat%20Insights%20Report%20Summer%202023.pdf