

# Around 50% of SMBs are facing cyberattacks and need customized solutions to secure their cyberspace

*SecureClaw is on the mission of cyber-securing SMBs worldwide with the BDSLCCI, Virtual CISO, VAPT, and various customized cybersecurity services and solutions.*

DOVER, DELAWARE, UNITED STATES, November 15, 2023 /

EINPresswire.com/ -- It is almost the end of the calendar year 2023. Even though the use of Chat-GPT and AI has increased worldwide, cyberattacks have also become more sophisticated

and have seen a significant increase. As Small and Medium Businesses (SMBs/SMEs) represent almost 90% of the business population, 60–70% of employment opportunities, and around 55% of the GDP contribution in developed economies, it is important to check how they are impacted by cyber threats.

“

SecureClaw believes that being cybersecure is the right of each organization, regardless of its domain, location, size, and revenue. Let SMB gain more confidence as a cyber-protected service provider.”

*Dr. Shekhar Pawar, CEO,  
SecureClaw Inc., Inventor of  
BDSLCCI*



The advertisement features a central image of a man in a white hoodie with the SecureClaw logo on the left, and a black hoodie with a Guy Fawkes mask on the right. The background is dark blue with a grid pattern. Text on the left reads: "ONE out of every TWO Small and Medium Businesses (SMBs / SMEs) is undergoing a cyberattack on average". Text on the right reads: "SecureClaw is on the MISSION of cybersecuring SMBs Worldwide with the BDSLCCI Cybersecurity Framework, Virtual CISO, VAPT, and various Customized Cybersecurity Services and Solutions". At the bottom, it says "SecureClaw Cybersecurity Services".

Below are a few important cyber-attack statistics related to SMBs since last year, which are the outcome of compiling various cyber threat reports, research, and cyber news that got [published on the SecureClaw Cyber Threat Advisory LinkedIn page](#).

1. In the past year, 50% of small and mid-sized firms said they had experienced at least one cyberattack.
2. According to Accenture's Cybercrime Survey, 43% of cyberattacks target small enterprises.
3. Six months after being the target of a cyberattack, 60% of small firms close their doors.

4. Of these reported SMBs, only 14% are ready for such an attack.

5. SMBs pay \$826 to \$653,587 on average for cybersecurity issues.

6. The cause of 95% of cybersecurity breaches is human mistake.

7. According to three out of four small enterprises, they lack the staff necessary to handle IT security.

8. 47% of small businesses don't know how to defend themselves from online threats.

9. Due to a cyber breach, forty percent of small and mid-sized firms had eight or more hours of unavailability.

10. Cybersecurity risk concerns 66% of small organizations, either very or very much.

11. Customer data compromise is the top issue for 66% of small firms.

12. Malicious emails affect small businesses 1 out of every 323 times.

13. Faulty systems and human mistake are to blame for 52% of data security incidents.

14. Following successful assaults, small enterprises must invest, on average, \$955,429 to get back to business as usual.

15. The cost of simply determining the source of a cyberattack might reach \$15,000.

16. The average cost of cyberattacks brought on by employee password compromises is \$383,365.

17. A quarter of small businesses were unaware of the financial consequences of cyberattacks.

18. 83% of small firms don't have any money set up to handle cyberattacks.

### SecureClaw's Virtual Chief Information Security Officer (V-CISO) Service

*YOU FOCUS ON YOUR BUSINESS FUNCTIONS*



**Virtual CISO**

**KEY BENEFITS:**

1. CISO role to display your clients and gain more confidence
2. Small Fixed Cost per month and extended service cost as per needs
3. Extensive Industry Knowledge and Skill
4. Guaranteed Objectivity
5. No Training & Certification Cost
6. Objective Measurable Performance
7. Access to team of Experts
8. Periodic cybersecurity assessment assistance, and much more...

**Specially Designed for Small and Medium Businesses (SMB / SME Companies)**

Virtual CISO Services by SecureClaw



### Static Application Security Testing (SAST Service)



Securing Your Organization's Cyberspace

Static Application Security Testing (SAST) by SecureClaw

19. 54% of small firms lack a plan for responding to cyberattacks.

20. Merely 14% of small businesses consider themselves highly effective in mitigating cyber dangers and assaults.

21. Costs associated with cybercrime are expected to rise by 15% over the next five years, to reach 10.5 trillion by 2025.

To improve cybersecurity posture of SMBs, SecureClaw Inc., is on the mission of providing tailored, less costly, and comprehensive services and solutions. Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI) framework platform, Virtual Chief Information Security Officer (Virtual CISO or V-CISO), Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and various other key services helps clients of SecureClaw to get security best practices deployed covering people, process, and technology areas.

#### [BDSLCCI Framework as a Service:](#)

It is a framework designed specifically for Small and Medium Enterprises (SMEs) that provides only the required minimum set of cybersecurity controls to be implemented depending on the business domain of the SMB. It is a new framework that provides a domain-specific security posture, which aids in the protection of the organization's important or mission critical asset areas. The BDSLCCI framework helps to prevent ransomware, malware, and various cyber threats in SMBs or SMEs by providing "tailored" cybersecurity controls based on the business domain of the organization, thereby "reducing the cost" of cybersecurity implementation by more than five times the cost of existing standards and providing many useful tools that are "free" to use.

#### Static Application Security Testing (SAST):

Static analysis, often known as static application security testing (SAST), is a testing approach that examines source code to discover security flaws that render the apps used by your company vulnerable to attack. White box testing is another name for it. SAST reduces the security risks in the application at a high level in the three phases of the software development life cycle (SDLC). Engineers who are creating and programming the application use SAST scans in their development process and tooling during development. Applications are released into production by going through the DevOps process, which results in production deployment. To guarantee that vulnerabilities are found before getting into production, SAST is also used at this phase. SAST is performed using tools and the manual source code review process.

#### Dynamic Application Security Testing (DAST):

Unlike SAST, DAST has no access to source code; rather, it has access to live applications or systems. Penetration testing is an active procedure that looks for potential vulnerabilities in active systems. Web applications today fuel a significant number of essential business operations, such as external e-commerce sites and internal finance systems. These web

applications can speed up corporate development, but they also often contain flaws that could result in a costly and disastrous data breach if they are not discovered and patched. Being a "Black box test" or "Gray box test," DAST runs independently of the program and lacks access to any internal source code or architectural specifications. Consequently, the test discovers vulnerabilities by launching an attack on the application using the same techniques a hacker would. In the global market, it is also well-known as vulnerability assessment and penetration testing, or VAPT. It is performed using various tools and manual test cases.

#### Virtual CISO:

An allocated resource with knowledge of creating and enhancing information security programs is referred to as a virtual CISO. A V-CISO first understands the benefits and drawbacks of an organization's security program by starting with a risk assessment. It is expensive to recruit a full-time CISO as well as a skilled team working with CISOs. SecureClaw is serving this role as a service. Many times, this role is shared among multiple skilled resources.

SecureClaw's team is working on a mission to build a good cybersecurity posture for every small and medium company.

Dr. Shekhar Pawar

SecureClaw Inc.

+ 12187182121

customercare@secureclaw.com

Visit us on social media:

[Facebook](#)

[Twitter](#)

[LinkedIn](#)

[Instagram](#)

[YouTube](#)

[Other](#)

---

This press release can be viewed online at: <https://www.einpresswire.com/article/668687084>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2023 Newsmatics Inc. All Right Reserved.