COGNNA

COGNNA'S SMALL AND MEDIUM-SIZED BUSINESSES THREAT REPORT 2024

TABLE OF CONTENTS

TABLE OF CONTENTS

03 INTRODUCTION

04 EXECUTIVE SUMMARY

05 THE ROLE OF SMES IN DRIVING THE ECONOMY OF SAUDI ARABIA

06 WHY ARE SMES MORE VULNERABLE TO CYBER ATTACKS?

08 DATA THEFT REMAINS THE PRIMARY OBJECTIVE

09 THE SME THREAT LANDSCAPE: HOW ARE SMES COMMONLY TARGETED?

- 09 RANSOMWARE
- 11 ADVANCED PERSISTENT THREATS (APTS)
- 12 BOTNETS
- 12 SUPPLY CHAIN EXPLOITS
- 12 INSIDER ATTACKS
- 12 SOFTWARE VULNERABILITY TARGETING
- 12 IDENTITY-BASED AND SOCIAL ENGINEERING ATTACKS

13 THREAT MITIGATION STRATEGIES FOR SMES AND COST CONSIDERATIONS

- 13 EMPLOYEE AWARENESS
- 13 THREAT IDENTIFICATION AND RESPONSE
- 14 REGULAR SECURITY AUDITS AND ASSESSMENTS
- 14 USER AUTHENTICATION AND ACCESS CONTROL
- 14 SOFTWARE UPDATES

15 CASESTUDY RANSOMWARE ATTACK ON A MID-SIZED CONSTRUCTION MANAGEMENT FIRM

- 15 OVERVIEW
- 15 TACTICS
- 15 TARGETED INDUSTRY
- 15 BUSINESS IMPACT
- 16 RESULTS AND RECOVERY

17 CASESTUDY RETAIL COMPANY'S BATTLE AGAINST VASHSORENA RANSOMWARE

- 17 OVERVIEW
- 17 TACTICS
- 17 TARGETED INDUSTRY
- 17 BUSINESS IMPACT
- 17 RESULTS AND RECOVERY

19 RECOMMENDATIONS

- 19 IMPLEMENT ROBUST BACKUP AND DISASTER RECOVERY SOLUTIONS
- 19 IMPROVE NETWORK SECURITY
- 19 DEPLOY ENDPOINT PROTECTION SOLUTIONS
- 19 ESTABLISH AN INCIDENT RESPONSE PLAN
- 19 MAKE CYBERSECURITY EVERYONE'S RESPONSIBILITY
- 19 IDENTIFY A RELIABLE CYBERSECURITY PARTNER

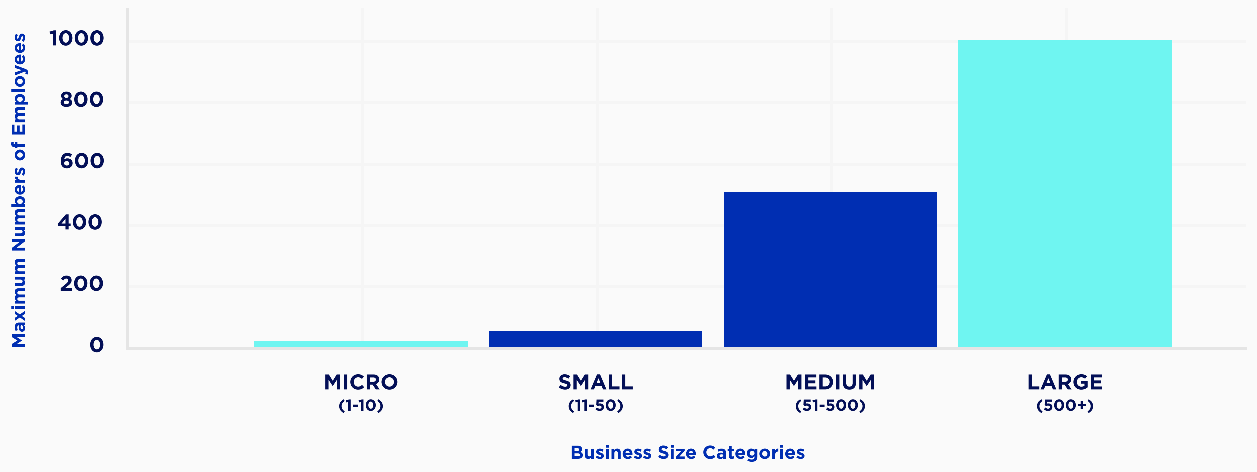
20 COGNNA'S THREAT DETECTION & RESPONSE PLATFORM

INTRODUCTION

INTRODUCTION

Globally, Small and Medium-sized Businesses (SMEs) or Small and Medium-sized Enterprises (SMEs) are typically defined as organizations that have **fewer than 500 employees.**

Classification of Business Sizes by the Number of Employees



Some resources stretch the definition to include **companies that have up to 1000 employees. In Saudi Arabia, SMEs** are defined as organizations that have **fewer than 250 employees** or **generate less than SAR200 million in revenue.**

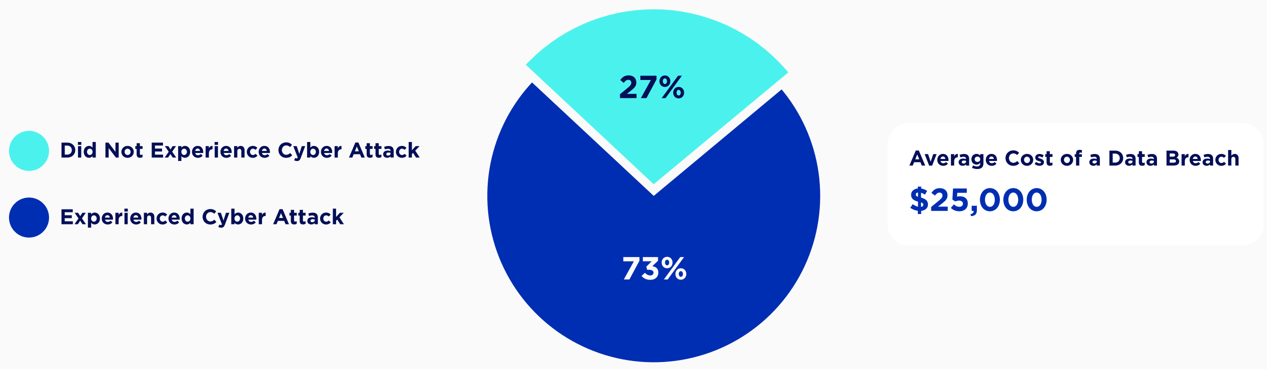
SMEs are the backbone of the Saudi economy, and despite lacking the same financial resources as large enterprises, they remain a prime target for cyber-criminals who want to get their hands on valuable customer data or infiltrate larger organizations in the same supply chain.

Cyberattacks that target SMEs rarely claim any major headlines, which led to the false assumption that **SMEs** are safe from malicious actors.

However, according to the ITRC's 2023 business impact report, **73% of SME business leaders** reported experiencing at least one cyber attack in the past year.

With each data breach costing small businesses $25,000 on average, such substantial damage can wreak havoc on the organization's business continuity.

Cyber Attack Experiences Among SME Business Leaders in the Past Year



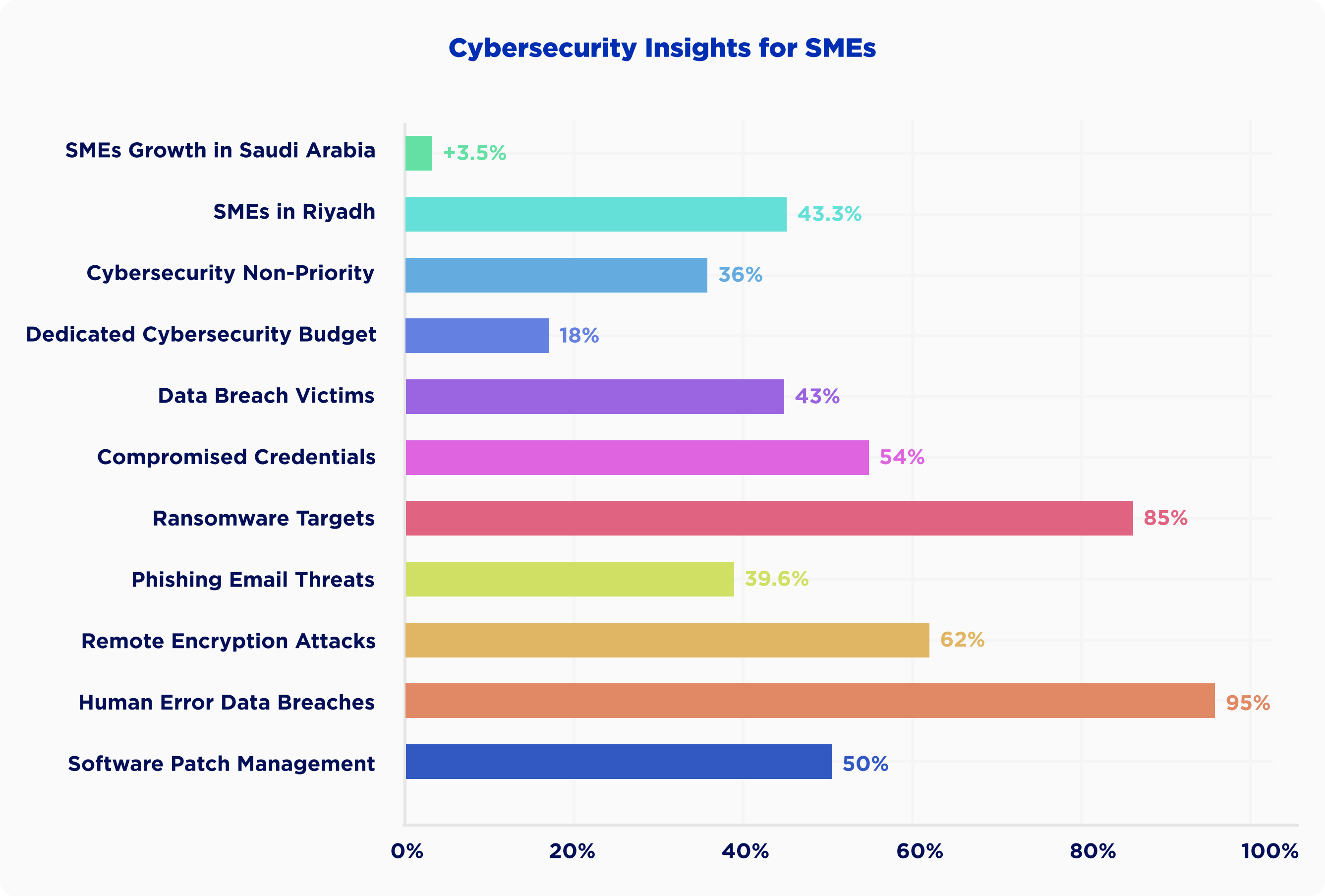
Despite these shocking numbers, **only 14% of SMEs are properly equipped to confront a cyberattack, leaving most SMEs vulnerable to cyber threats.**

IN COGNNA'S 2024 CYBERSECURITY ADVERSARY REPORT

We will explore the threat landscape for small and medium-sized enterprises, covering the current security trends and how to make your small business prepared against rising threats.

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY



The number of SMEs in Saudi Arabia increased by 3.5%, bringing the total count to 1.27 million businesses.

Riyadh is now home to 43.3% of small and medium-sized businesses.

36% of small business leaders believe that cybersecurity isn't a priority concern for them at all.

Only 18% of mid-sized organizations with 250+ employees have a dedicated cybersecurity budget.

43% of data breach victims are small businesses.

54% of data breaches against SMEs resulted in compromised credentials.

85% of ransomware attacks are targeted at small businesses.

Phishing is the most common form of email threats, standing at 39.6% of all email threats.

Remote encryption is one of the most common ransomware attack vectors, accounting for 62% of ransomware attacks on small businesses.

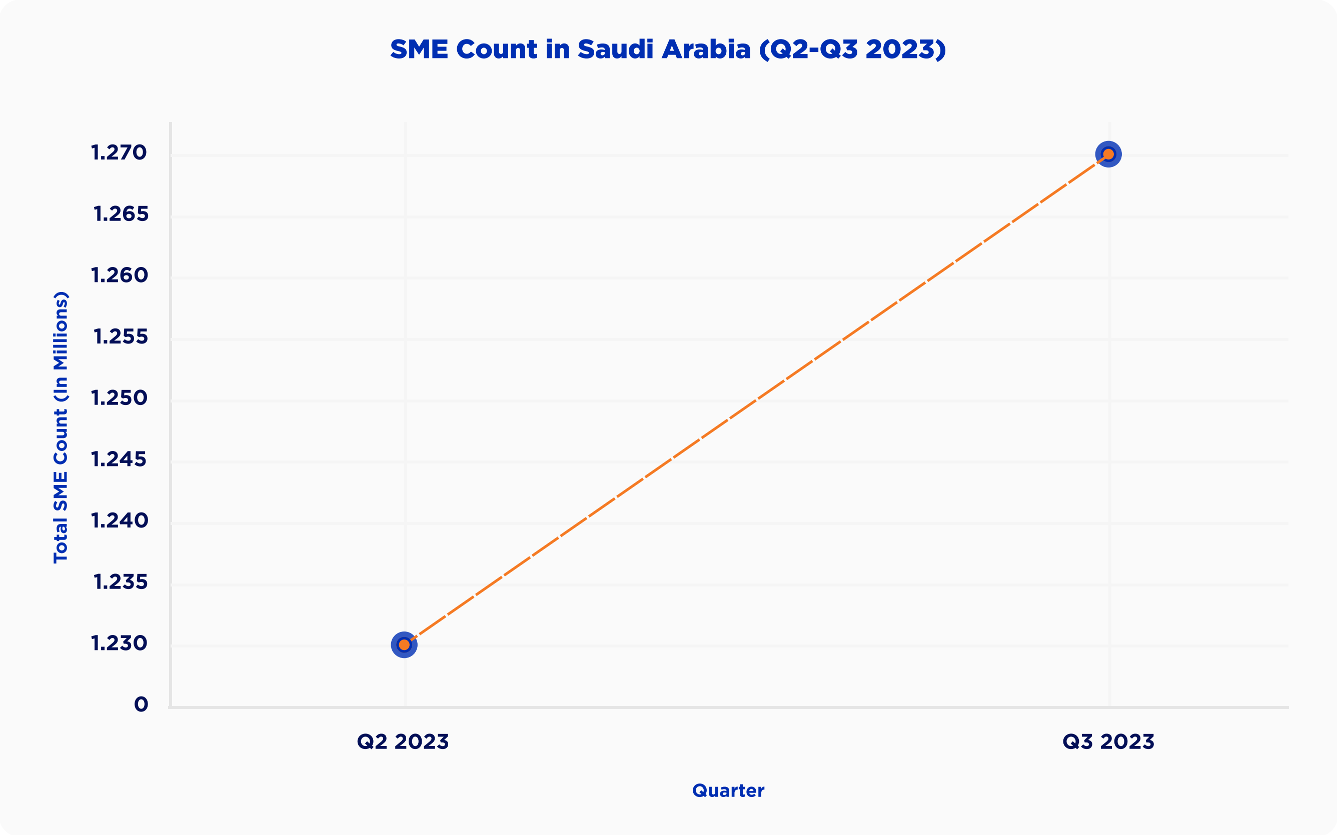
95% of data breaches are caused by human error. Employee training and awareness can help mitigate this threat.

Only 50% of small business leaders have a documented software patch management process.

THE ROLE OF SMES IN DRIVING THE ECONOMY OF SAUDI ARABIA

THE ROLE OF SMES IN DRIVING THE ECONOMY OF SAUDI ARABIA

Small and Medium-sized Enterprises (SMEs) play a vital role in driving the economy of Saudi Arabia. **In Q3 2023 alone, the kingdom witnessed a substantial surge in SMEs, with a notable 3.5% increase, bringing the total count to a staggering 1.27 million.**


SME Count in Saudi Arabia (Q2-Q3 2023)

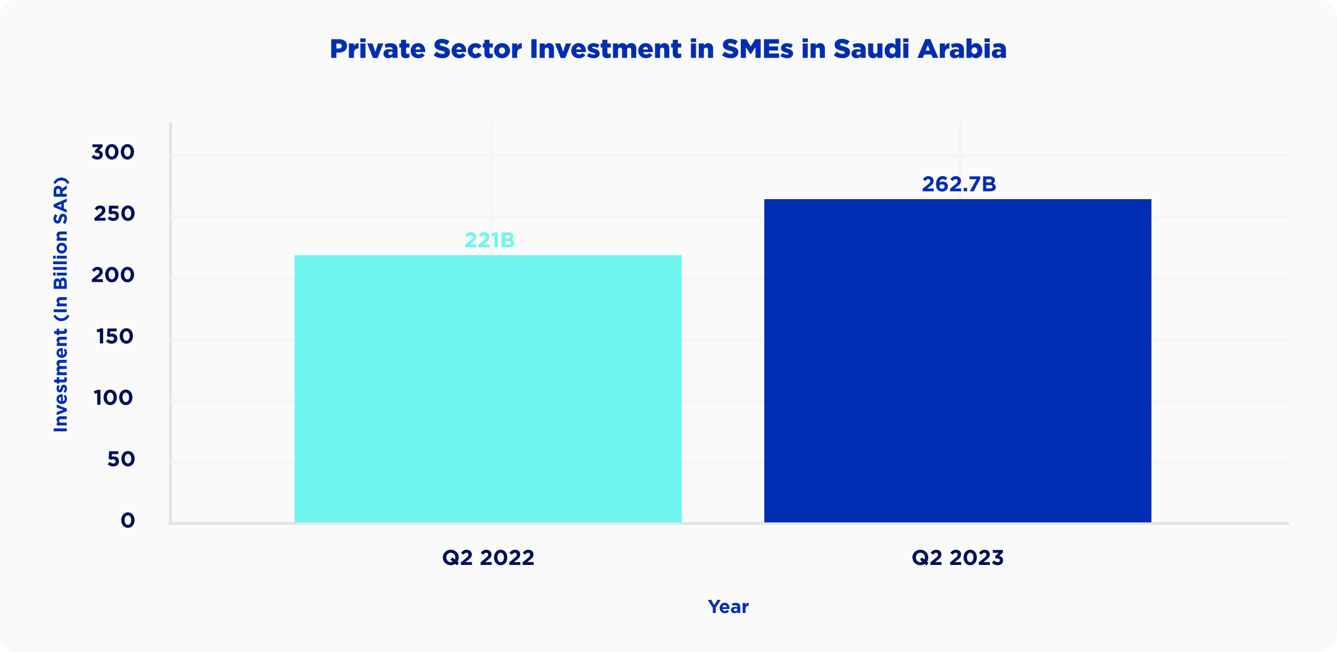
Over **40,000 new businesses were launched across various sectors**, indicating a vibrant entrepreneurial environment within the country.

The Capital, Riyadh, has evolved into a focal point for startup SMEs in Saudi Arabia, **housing 43.3% of these businesses.**

Moreover, **the growth of the manufacturing sector by 4.6% year-on-year in Q3 2023** is indicative of SMEs' expanding footprint in industrial and manufacturing spaces, accelerated by initiatives such as the **National Industrial Development and Logistics Program (NIDLP) and other government initiatives.**

Such initiatives have facilitated the entry of more SMEs into these sectors and contributed to the overall economic diversification agenda of the kingdom.

Highlighting the confidence of private investors in the resilience and potential of SMEs in the kingdom, **the private sector investment witnessed a significant 18.8% year-on-year increase in Q2 2023, amounting to SAR262.7 billion ($70 billion).**


Private Sector Investment in SMEs in Saudi Arabia

WHY ARE SMES MORE VULNERABLE TO CYBER ATTACKS?

WHY ARE SMES MORE VULNERABLE TO CYBER ATTACKS?

Contrary to popular belief, small businesses are not immune to cyber threats. In fact, **they are more vulnerable than larger corporations,** and in many cases, **the business impact can be disproportionately severe.**

One primary reason cyber attackers target SMEs is the valuable data they possess. Despite their size, many small businesses hold significant volumes of customer payment data and other sensitive information, **making them a lucrative target for hackers seeking financial gain or aiming to exploit it for further malicious activities.**

Furthermore, SMEs often lack the necessary cyber security and IT budget needed to implement reliable cybersecurity measures and incident response plans that larger enterprises have in place, **making them easy prey for cybercriminals to breach.**

SMES ARE MORE VULNERABLE THAN LARGER CORPORATIONS DUE TO:

SMEs hold significant volumes of customer payment data and other sensitive information.

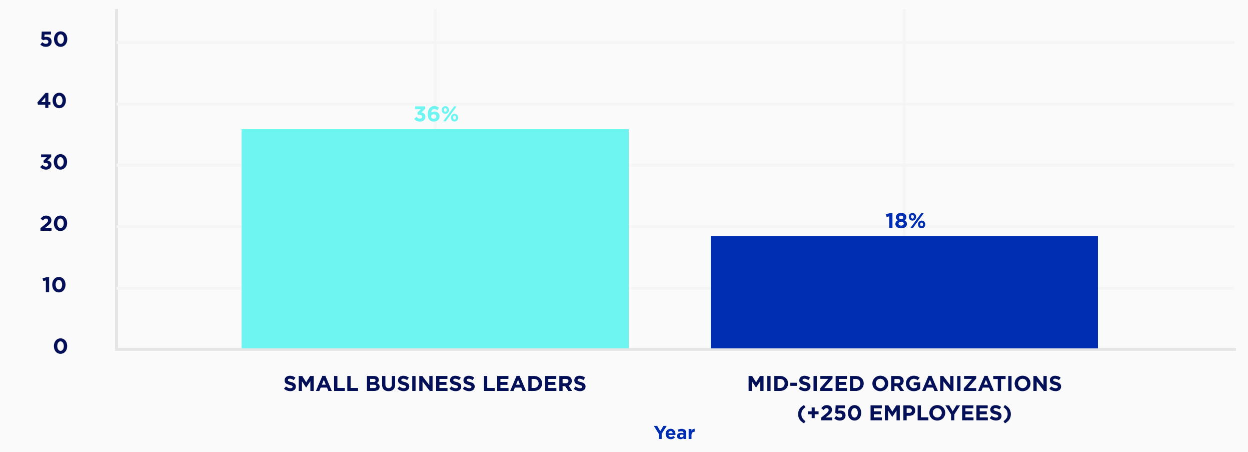
Lack of the necessary cyber security and IT budget.

The misconception among SME business leaders that they are unlikely to be targeted by cyber criminals.

Another contributing factor to the vulnerability of SMEs is the common misconception among SME business leaders that **they are unlikely to be targeted by attackers, creating a false sense of security.**

36% of small business leaders believe that cybersecurity isn't a concern for them at all, and only **18% of mid-sized organizations with 250+ employees allocate a cybersecurity budget.**

Concern and Budget Allocation Towards Cybersecurity



WHY ARE SMES MORE VULNERABLE TO CYBER ATTACKS?

WHY ARE SMES MORE VULNERABLE TO CYBER ATTACKS?

As a result, SME business owners prioritize investing in business growth initiatives while neglecting cybersecurity measures.

Limited budget allocations, reliance on outdated systems, and lack of cybersecurity training for employees further compound the vulnerability of small businesses to cyber threats.

Additionally, the increased adoption of remote and hybrid work environments has made SMEs more vulnerable to cyber attacks that target loosely secured endpoints and use them to infiltrate the company's broader network.

With employees using personal devices and relying on cloud services without sufficient IT support, small businesses have become more susceptible to cyberattacks like social engineering scams and malware infiltration.

The impact of cyberattacks on small businesses includes both direct and indirect costs.

Direct costs encompass financial losses and hindered business operations, while indirect costs comprise damaged reputation, loss of customer and stakeholder trust, and lowered team morale.

Moreover, cyberattacks can lead to price increases for consumers as businesses seek to offset the financial losses incurred, which can further deteriorate the customers' relationship with your brand and drive them towards competitors offering more reasonable prices and better security measures.

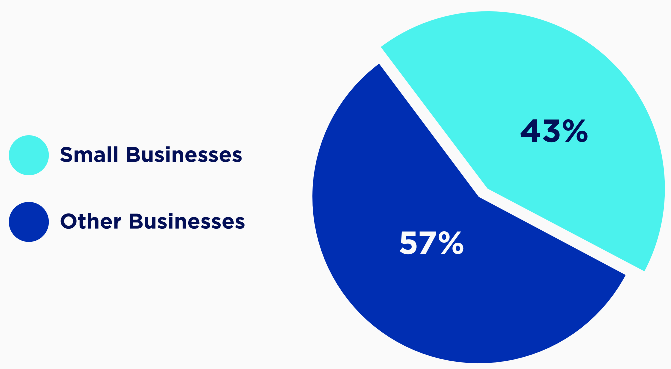
Additionally, the damage to a business's reputation resulting from a cyberattack can have long-lasting impressions, driving away potential customers, investors, and qualified job seekers.

DATA THEFT REMAINS THE PRIMARY OBJECTIVE

DATA THEFT REMAINS THE PRIMARY OBJECTIVE

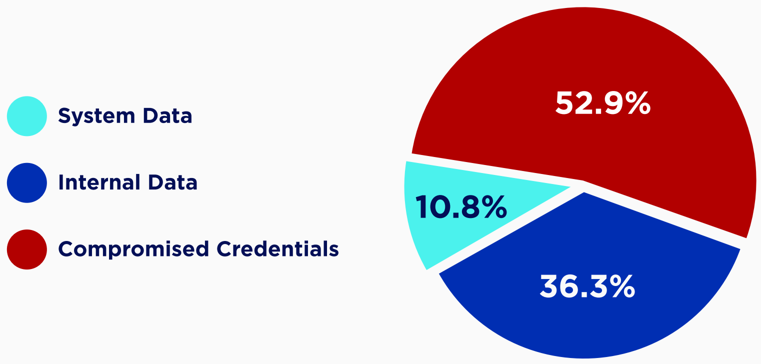
Data theft remains a primary target for cyber attacks **directed at SMEs,** with **43% of recorded data breach victims being small businesses.**

Proportion of Data Breach Victims by Business Size



Further, based on recent research, **54% of data breaches against SMEs resulted in compromised credentials, followed by internal data (37%), and system data (11%).**

Types of Data Compromised in SME Breaches



Most threat actors that targeted SMEs had financial motives (98%), compared to **just 1% for espionage.**

THE SME THREAT LANDSCAPE: HOW ARE SMES COMMONLY TARGETED?

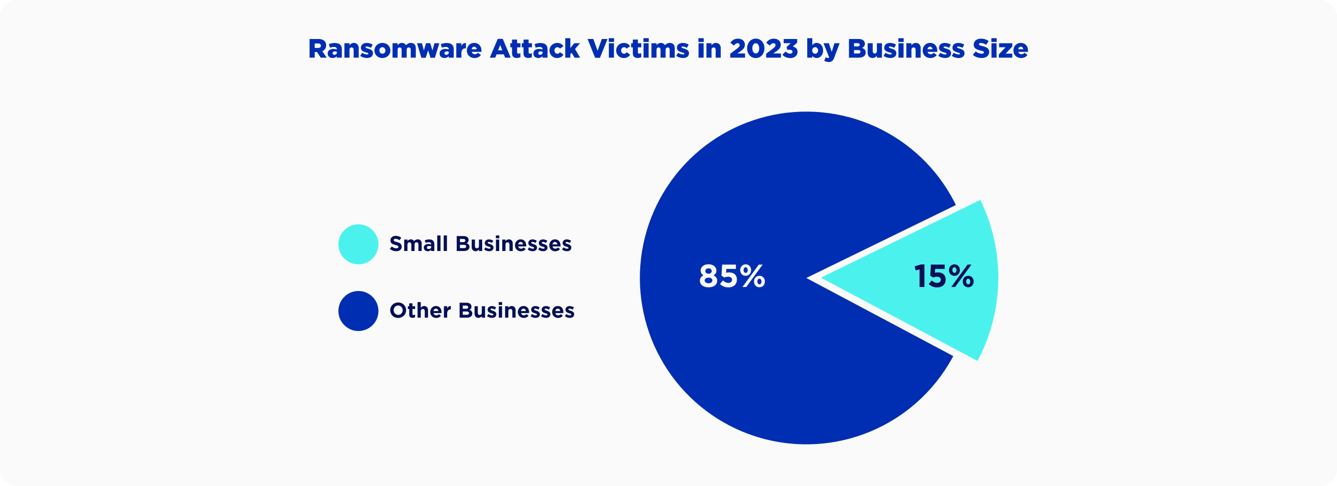
THE SME THREAT LANDSCAPE: HOW ARE SMES COMMONLY TARGETED?

Threat actors can target SMEs in different ways, Many of the techniques they employ are evolving, meaning that they get more sophisticated **over time as they adapt to cyber security measures employed by organizations.**

A CYBERATTACK ON A SMALL BUSINESS CAN TAKE ANY OF THE FOLLOWING FORMS:

- **Ransomware**
- **Advanced Persistent Threats (APTs)**
- **Botnets**
- **Supply Chain Exploits**
- **Insider Attacks**
- **Software Vulnerability Targeting**
- **Identity-based and Social Engineering Attacks**

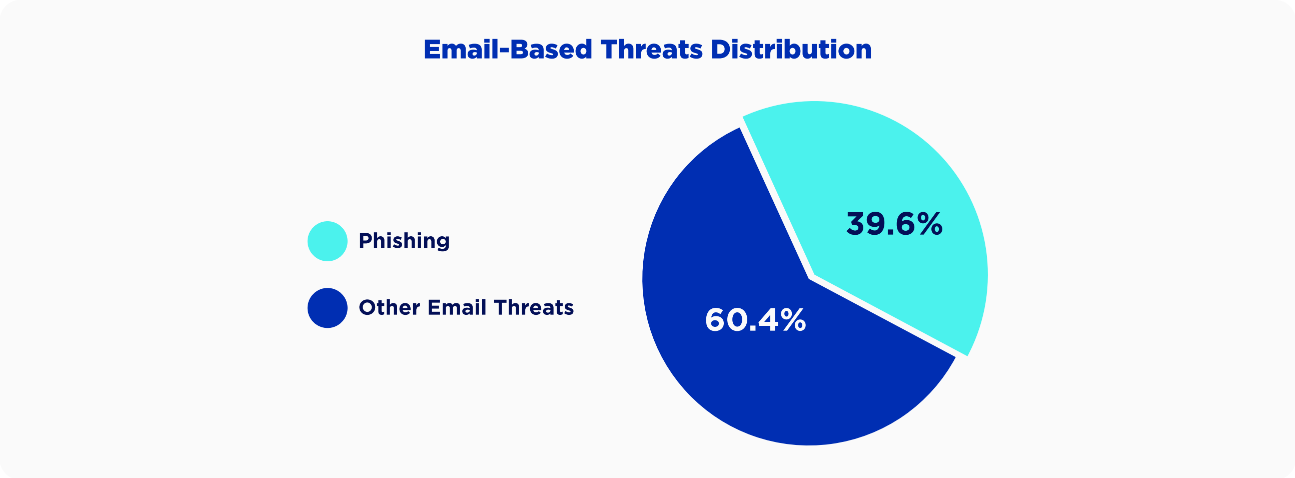
1. RANSOMWARE


Ransomware Attack Victims in 2023 by Business Size

For SMEs, ransomware remains the most common type of malware that targets SMEs. **According to Veeam's data protection trends report, 85% of ransomware attack victims in 2023 were small businesses.**

- **Cybercriminals commonly employ one of the following attack vectors to encrypt the mission-critical data of the victims:**

1. Phishing:


Email-Based Threats Distribution

Phishing is an identity-based ransomware attack where a malicious user sends an email to a legitimate user while falsely claiming to be a trusted person or entity. The cybercriminal typically asks the user to submit their login credentials so they can access sensitive data and encrypt it. Currently, phishing is considered the most common email-based threat, accounting for 39.6% of all email threats.

THE SME THREAT LANDSCAPE: HOW ARE SMES COMMONLY TARGETED?

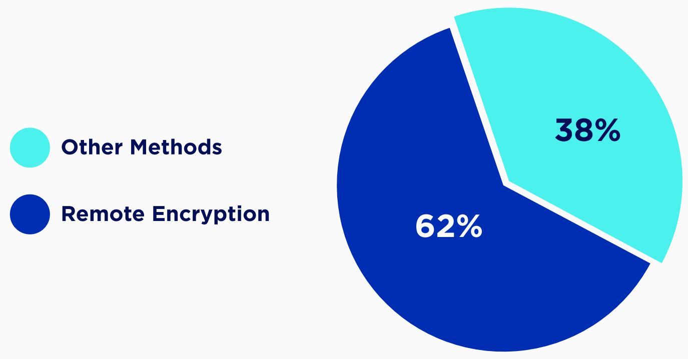
2. **Brute-force Attack:**

   A brute-force attack comprises the threat actor using decryption software to compromise user credentials. They also involve purchasing the stolen credentials from other criminal sites.

3. **Software Vulnerability:**

   When the company's software is out of date and unpatched, the threat actor exploits the vulnerability to deploy ransomware and encrypt data.

Ransomware Attack Methods on SMEs



A well-known ransomware type that has primarily targeted SMEs is LockBit. Akira and BlackCat have also repeatedly launched campaigns on small businesses. A common tactic they employ is remote encryption, which takes advantage of unmanaged devices on the company's network to encrypt sensitive data on other systems. **At least 62% of ransomware attacks on SMEs leveraged remote encryption to compromise valuable data.**

THE SME THREAT LANDSCAPE: HOW ARE SMES COMMONLY TARGETED?

2. ADVANCED PERSISTENT THREATS (APTS)

Advanced Persistent Threats (APTs) are strategic cyberattacks conducted by state-linked or organized criminal groups.

Recently, APTs have intensified their focus on SMEs, aiming to exploit vulnerabilities in the supply chain and gain access to larger targets. Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) warns that APTs are targeting Managed Service Providers **(MSPs).**

APT threat actors utilize attack vectors such as phishing campaigns, targeted attacks on **SMEs in the financial sector, and supply chain exploitation.**

Common APT tactics include long-term, multi-staged attacks, supply chain exploitation, use of custom malware and zero-day vulnerabilities, establishment of Command and Control (C2) servers, lateral network movements, and data exfiltration.

- **A successful APT attack progresses through three stages:**

1. Infiltration:

Infiltration occurs through compromised web assets, network resources, or authorized users.

2. Expansion:

Expansion involves targeting higher-level personnel and acquiring sensitive data, potentially for sabotage.

3. Extraction of Stolen Data:

Threat actors distract security teams with tactics like DDoS attacks to facilitate data removal undetected.

One example is APT34, a threat actor engaged in a protracted cyber espionage campaign primarily centered on reconnaissance activities.

The threat group has undertaken widespread targeting across various industries, encompassing financial, government, energy, chemical, and telecommunications sectors.

Their operations have predominantly concentrated within the Middle East.

In its most recent campaign, APT34 exploited the recent Microsoft Office vulnerability CVE-2017-11882 to deploy POWRUNER and BONDUPDATER, affecting SMEs that use MS Office.

To combat these threats, SMEs and MSPs are advised to implement security measures such as adopting CISA's recommendations for Microsoft services, segregating administrator accounts, and closely monitoring access logs.

THE SME THREAT LANDSCAPE: HOW ARE SMES COMMONLY TARGETED?

THE SME THREAT LANDSCAPE: HOW ARE SMES COMMONLY TARGETED?

3. BOTNETS

A botnet comprises a large network of compromised devices that are controlled by one entity. The term botnet is a combination between the words "robot" and "network". When a new device is compromised, it automatically gets added to the network.

- **Botnets target SMEs in multiple ways:**

  1. **Distributed Denial-of-Service (DDoS) attacks:**

     The botnet floods an organization's website with an unusual flow of traffic until it crashes and becomes inaccessible to actual users. The purpose behind DDoS attacks is to damage the company's reputation and induce financial losses.

  2. **Data Theft:**

     Bots can be programmed to steal sensitive information like customer credit card data, leading to severe financial and legal consequences for SMEs.

  3. **Spam and Phishing:**

     Botnets can be used to spam employee email inboxes with large amounts of emails that contain phishing links, which may cause employees to accidentally submit sensitive information and credentials.

4. SUPPLY CHAIN EXPLOITS

Most of the time, SMEs aren't the primary targets of supply chain attacks. While supply chain threats pose a higher risk for larger enterprises, cybercriminals may initially attack an SME that shares the same supply chain as other bigger corporations and use the vulnerability as a backdoor to infiltrate their network.

5. INSIDER ATTACKS

Insider attacks are often neglected, but they can be a more significant risk than many external threats. An insider attack can either be intentional or unintentional. One example of an immoral attack is when a terminated employee steals the company's sensitive data and sells it to external actors on their last day on the job.

On the other hand, an unintentional insider attack is when an employee with privileged access permissions accidentally leaks sensitive data, either through data input error or a phishing email, for instance.

6. SOFTWARE VULNERABILITY TARGETING

Threat actors exploit software vulnerabilities to infiltrate the networks of small businesses.

Ideally, software vulnerabilities are identified and patched quickly, but in reality, this isn't always the case. **In fact,** some software vulnerabilities persist for years without being discovered, providing opportunities for malicious actors to breach systems and steal valuable data.

SMEs are even more vulnerable to software vulnerability attacks because they often don't have a strict patch management and software update procedure, leaving their systems exposed to threats.

In a recent survey, **only half of small business leaders thought that their patch management process was robust enough to protect them against cyber attacks.**

7. IDENTITY-BASED AND SOCIAL ENGINEERING ATTACKS

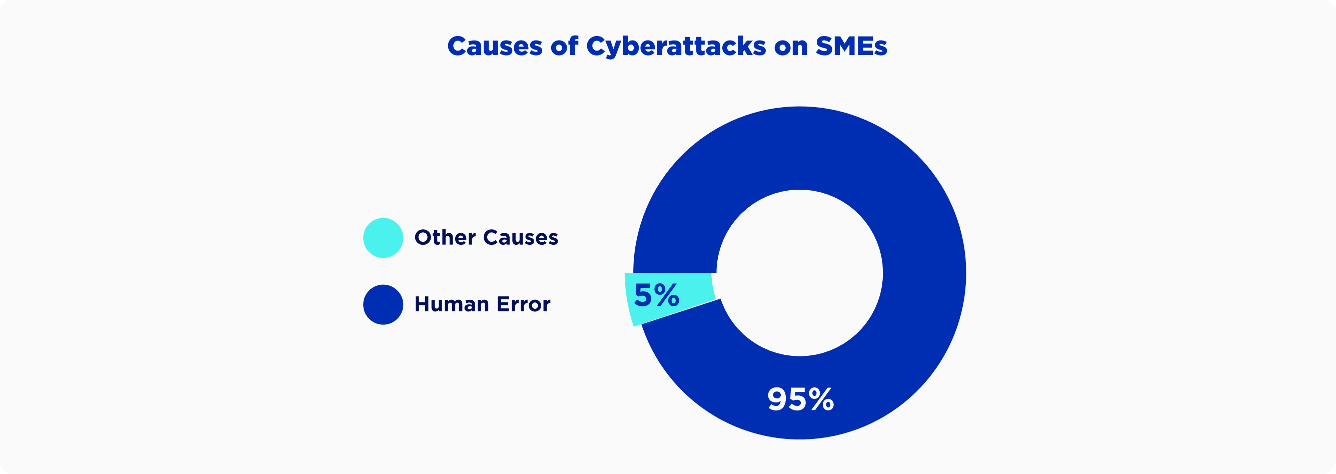
An identity-based attack starts with a malicious user pretending to be a top-level employee or executive at the company, either through phishing or compromised accounts.

The attacker then uses social engineering techniques to manipulate or persuade company officials into submitting sensitive information.

THREAT MITIGATION STRATEGIES FOR SMES AND COST CONSIDERATIONS

To minimize the risk of cyberattacks on your SME, you need to invest in multiple threat mitigation strategies. These include:

1. EMPLOYEE AWARENESS



The lion's share of cyberattacks on SMEs can be traced back to a lack of employee awareness, with the World Economic Forum **attributing 95% of breaches to human error.**

Increasing employee awareness with security training sessions and mock attacks can enhance their ability to identify threats and prevent attacks from happening in the first place.

For example, you can incorporate randomly-timed phishing tests to gauge each employee's ability to identify phishing emails. **It's also important to create and enforce strict cybersecurity policies that discuss essential data protection strategies throughout your entire organization.**

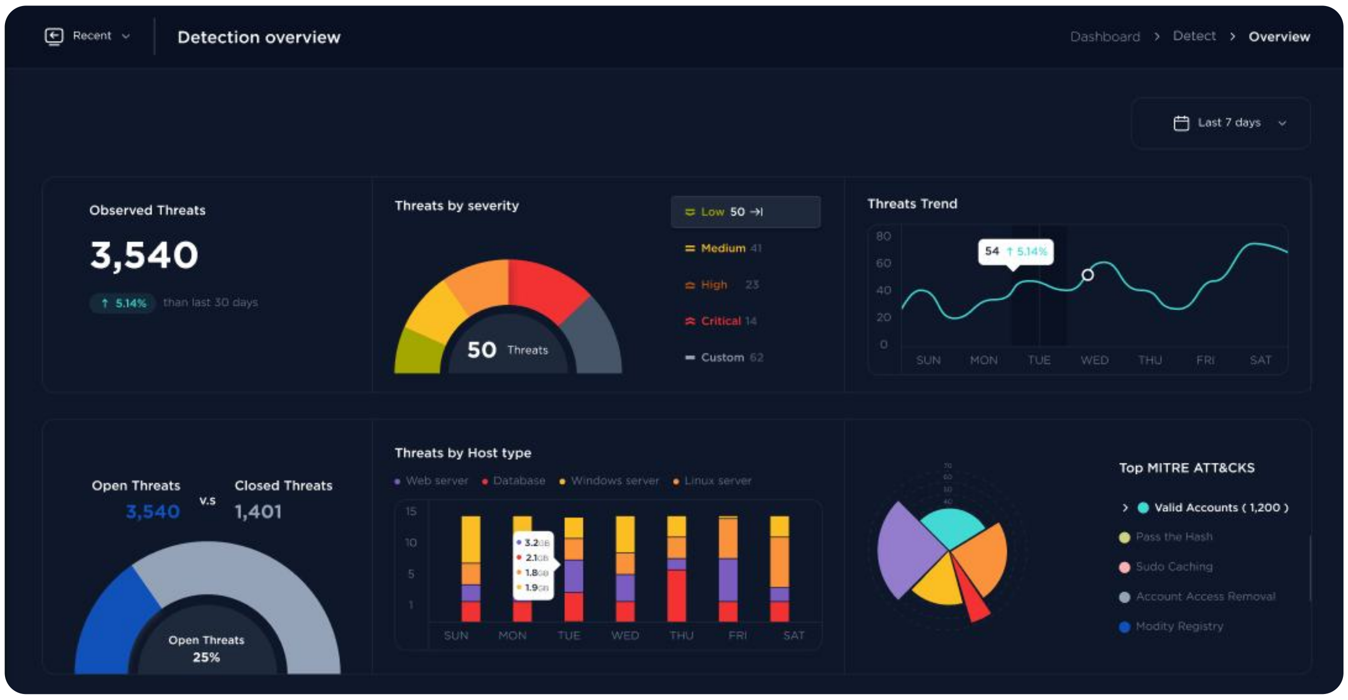
Security training is one of the most cost-efficient ways to protect your organization against cyber threats, but if your IT staff is already at full capacity, **you might consider hiring more staff to accommodate your training needs.**

2. THREAT IDENTIFICATION AND RESPONSE

Proactively detecting and responding to cyber threats enables you to stay one step ahead of threat actors targeting your organization. Instead of responding to cyber attacks after the damage is done, the threat identification and response process relies on discovering vulnerabilities and mitigating threats before they lead to data breaches or system compromise.

However, this approach can be costly as you will need to invest in infrastructure and technology. You will also have to expand your IT team.

Leveraging COGNNA Threat Detection and Response can address the gap by identifying threats, and providing automated detection and response workflows to address challenges that SMEs face.



THREAT MITIGATION STRATEGIES FOR SMES AND COST CONSIDERATIONS

THREAT MITIGATION STRATEGIES FOR SMES AND COST CONSIDERATIONS

3. REGULAR SECURITY AUDITS AND ASSESSMENTS

Investing in regular security audits can help you identify vulnerabilities and maintain compliance with regulatory standards, potentially preventing costly breaches in the long run. Security audits and assessments can be internal or external.

Internal audits may be more cost-effective, but they are not enough to properly assess your security readiness. They are typically used as a preliminary step to a more extensive audit by an external auditor. **Costs may vary based on the depth and frequency of audits, but they'll definitely add significant expenses to your monthly budget.**

4. USER AUTHENTICATION AND ACCESS CONTROL

Implementing strict user authentication methodologies is crucial to prevent fraud and mitigate identity-based cyber threats, enabling you to minimize the attack surface for threats and contain damage in case of data breach.

However, this may require high initial setup costs. You should also consider the ongoing maintenance and support for access control systems, which can add to the expenses. Balancing security with user convenience is also crucial since overly complicated authentication methods often lead to lost productivity.

Further, it's important to develop a no-trust mindset based on the **zero-trust security model.** The foundational concept of this model is that no user should be fully trusted and that breach is always a highly likely occurrence. You can maintain strict user permission controls by giving each user the least possible access privileges for them to carry out their job functions.

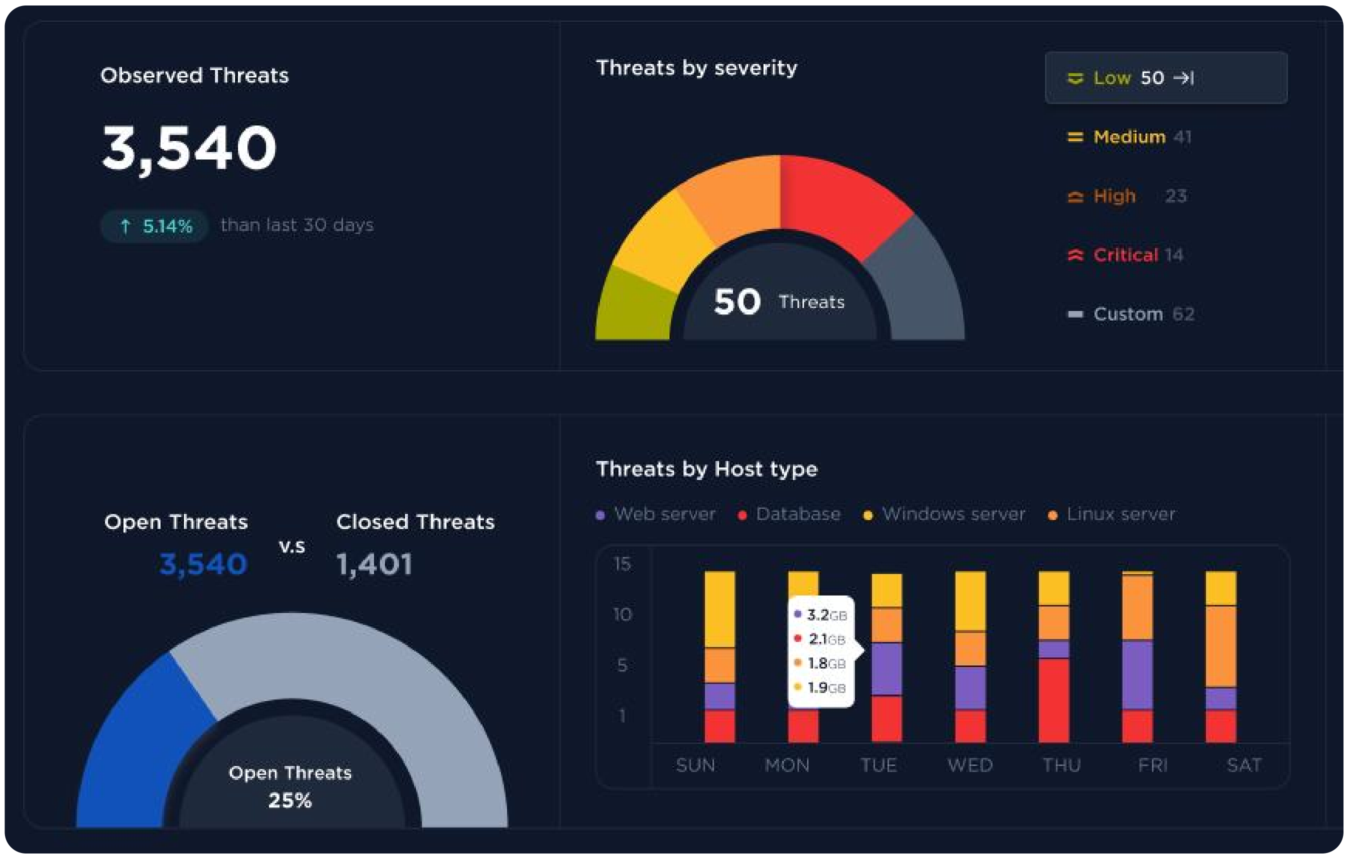
5. SOFTWARE UPDATES

Keeping your software up-to-date is an essential and cost-effective way to mitigate cyber threats. Most cyber criminals rely on zero-day exploits to compromise the networks of SMEs.

As a result, updating your software as soon as a new security or vulnerability patch is released is vital.

However, you should consider the cost of testing and implementing these software updates, especially if you run proprietary software.

Leveraging COGNNA Identify module helps identifying the vulnerable assets and missing patches, by providing a comprehensive analysis of the vulnerability status across all systems in the organization.



CASE STUDY
RANSOMWARE ATTACK ON A
MID-SIZED CONSTRUCTION
MANAGEMENT FIRM

CASESTUDY

RANSOMWARE ATTACK ON A MID-SIZED CONSTRUCTION MANAGEMENT FIRM

OVERVIEW

- A mid-sized construction management firm found itself at the mercy of a debilitating ransomware attack, disrupting operations and causing significant financial losses.
- With 50 employees reliant on computer systems for daily tasks ranging from project management to financial tracking, the attack paralyzed the company's ability to function efficiently.
- The ransomware attack compromised their internal workstations and backups. It rendered the company's existing network security and data backup systems inadequate, leaving crucial data inaccessible and operations halted.

TACTICS

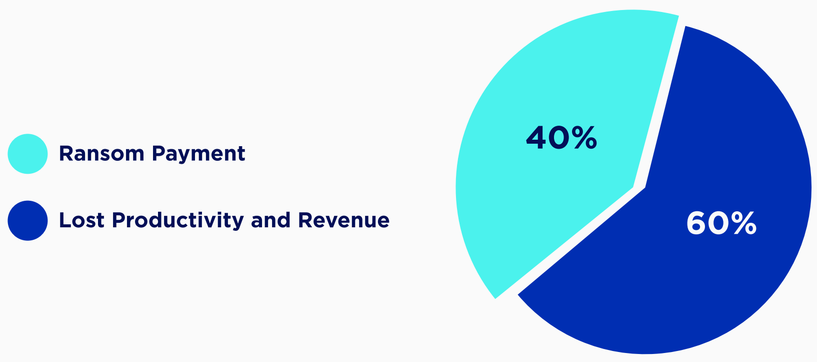
- The attackers exploited vulnerabilities in the firm's network security, likely infiltrating through phishing emails or unpatched software.
- Once inside the network, they deployed ransomware, encrypting critical data and demanding payment for its release.
- The company's lack of robust backup protocols left them with no option but to negotiate with the attackers, resulting in a substantial ransom payment.

TARGETED INDUSTRY

- The construction industry, although traditionally focused on physical infrastructure, is increasingly reliant on digital technologies for project management, communication, and financial transactions.
- The victim's reliance on networked systems made them a prime target for cybercriminals seeking to exploit vulnerabilities in both their technology and data management practices.

BUSINESS IMPACT

Financial Impact of Ransomware Attack on Construction Management Firm



- **The ransomware attack** had devastating consequences for the construction management firm, resulting in **over $200,000 in financial losses.**
- **This included** the ransom payment of **$80,000 in cryptocurrency and an additional $120,000 in lost productivity and revenue during the 14 days of downtime.**
- **Moreover,** the company's reputation suffered a blow as clients experienced delays and disruptions to ongoing projects.

CASE STUDY
RANSOMWARE ATTACK ON A MID-SIZED CONSTRUCTION MANAGEMENT FIRM

RANSOMWARE ATTACK ON A MID-SIZED CONSTRUCTION MANAGEMENT FIRM

RESULTS AND RECOVERY

- The construction management firm turned to a cyber security solutions provider for assistance in mitigating the effects of the attack and restoring normal operations.
- Leveraging their expertise in cybersecurity and data recovery, the third-party solution provider eradicated the ransomware threat and restored access to encrypted data within 48 hours.
- **Furthermore,** the provider implemented robust security measures to fortify the construction firm's network against future attacks, including regular security audits, employee training on identifying phishing scams, and the establishment of secure backup protocols.

CASE STUDY RETAIL COMPANY'S BATTLE AGAINST VASHSORENA RANSOMWARE

CASESTUDY

RETAIL COMPANY'S BATTLE AGAINST VASHSORENA RANSOMWARE

OVERVIEW

- In October 2023, a prominent retail sector company faced an unprecedented cybersecurity challenge when it fell victim to a sophisticated ransomware attack.
- The attackers deployed the Vash Sorena ransomware, targeting the company's network infrastructure and encrypting critical data.
- As a result, the company's financial system and employee computers were rendered inaccessible, leading to a complete shutdown of operations across more than 8 branches.
- The attack exploited vulnerabilities in the company's network infrastructure, allowing the perpetrators to infiltrate its systems and deploy the VashSorena ransomware.

TACTICS

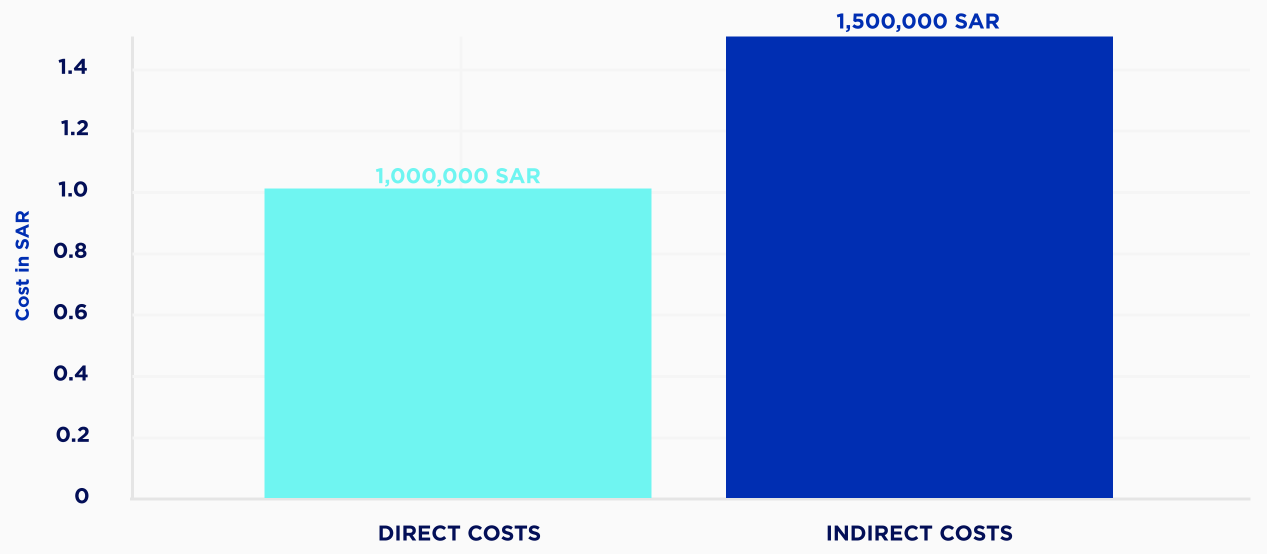
- The threat actor initiated the breach by exploiting a public-facing vulnerability in Remote Desktop Protocol (RDP), a commonly used protocol for remote access to computer systems.
- Upon breaching the company’s network, the attackers deployed a customized malware variant designed to propagate rapidly across the network, encrypting critical files and locking down essential systems.

TARGETED INDUSTRY

- The retail industry, which relies heavily on digital technologies for inventory management, sales transactions, and customer engagement, was specifically targeted in this cyberattack.
- The attackers aimed to disrupt the company's operations and compromise its financial integrity by encrypting vital data stored within its network infrastructure.

BUSINESS IMPACT

Financial Impact of Ransomware Attack on Retail Company



- The ransomware attack had severe consequences for the retail company, resulting in a complete paralysis of operations across all branches for a duration of two weeks.
- With the company's financial system and employee computers incapacitated, essential business processes were disrupted.
- The direct costs incurred for data recovery, system restoration, and cybersecurity enhancements amounted to more than 1M SAR.
- Additionally, the company suffered significant losses due to the inability to operate for two weeks and the lack of records pertaining to receivable payments.

CASE STUDY
RETAIL COMPANY'S BATTLE AGAINST VASHSORENA RANSOMWARE

RETAIL COMPANY'S BATTLE AGAINST VASHSORENA RANSOMWARE

RESULTS AND RECOVERY

- **Following the cyberattack,** the retail company embarked on a comprehensive response and recovery effort to mitigate the impact of the ransomware attack.
- **Partnering with COGNNA,** the organization invested in cybersecurity measures that include regular vulnerability assessments, threat detection and mitigation, and employee training programs focused on cybersecurity awareness and best practices.

RECOMMENDATIONS

Small businesses are prime targets for cyberattacks, but with some proactive measures, you can significantly reduce your risk. These are our recommendations to prevent and mitigate cyberattacks:

1. IMPLEMENT ROBUST BACKUP AND DISASTER RECOVERY SOLUTIONS

- Create frequent backups of critical data and store them in an off-site location inaccessible to attackers.
- Regularly test the backups to verify their integrity and effectiveness in restoring operations in case of a disaster.

2. IMPROVE NETWORK SECURITY

- Conduct regular vulnerability assessments and penetration testing to identify and address weaknesses in your network infrastructure.
- It's also important to use multi-factor authentication (MFA) for authenticating users to add an extra layer of security to accounts, especially if you have a remote or hybrid work environment.

3. DEPLOY THREAT DETECTION AND RESPONSE SOLUTIONS

- Deploying threat detection and response solutions is essential for enhancing your security posture, especially in remote and hybrid work environments.
- With a capable threat detection and response solution, you can protect your endpoints against potential threats with proactive threat detection, real-time threat intelligence and monitoring, and rapid response.

4. ESTABLISH AN INCIDENT RESPONSE PLAN

- Develop a comprehensive incident response plan outlining roles, responsibilities, and procedures to follow in case of a cyberattack.
- Test the incident response plan regularly through tabletop exercises and simulations to ensure effectiveness and readiness to respond to cyber incidents.

5. MAKE CYBERSECURITY EVERYONE'S RESPONSIBILITY

- Cybersecurity shouldn't be the responsibility of your security staff only.
- Everyone in your organization should be held accountable, from employees to managers and CTOs.

6. IDENTIFY A RELIABLE CYBERSECURITY PARTNER

- Partner with a reputable cybersecurity solution provider like COGNNA to evaluate your security posture, identify security gaps, and implement tailored security measures to mitigate the risk of cyberattacks.
- With managed security services, you'll be able to continuously monitor and manage security threats and respond effectively to incidents, all while keeping costs in check.

COGNNA'S THREAT DETECTION & RESPONSE PLATFORM

COGNNA offers a unified platform that combines managed services, local support, and cost efficiency.

With COGNNA, your most complex cybersecurity operations become simpler, all while ensuring maximum protection and adherence to regulatory compliance requirements.

Our platform boasts advanced threat detection capabilities, incorporating cutting-edge vigilant monitoring and rapid response tools. COGNNA also provides actionable intelligence to quickly identify and neutralize threats, supported by accurate security logging from your on-premises and cloud environments.

OUR CYBERSECURITY EXPERTS EMPLOY PATTERN RECOGNITION TO IDENTIFY THREATS EFFECTIVELY. WHEN ANALYZING CYBER INCIDENTS, WE LOOK FOR CONSISTENT PATTERNS SUCH AS:

Our cybersecurity experts employ pattern recognition to identify threats effectively. When analyzing cyber incidents, we look for consistent patterns such as:

- Similar tactics, techniques, and procedures (TTPs) that are used across multiple attacks.
- Common infrastructure utilized by threat actors.

It's not uncommon for multiple threat actors to claim credit for the same attack. In such cases, threat actors may make claims to enhance their reputation, attract sponsors, or divert attention from the actual perpetrator.

At COGNNA, we delve deep into the intricacies of cyber incidents to uncover the truth behind the claims and identify the responsible threat actors accurately.

Moreover, we offer a streamlined threat identification, response, and recovery process, supporting your business continuity with effective incident management and risk mitigation techniques.

COGNNA also deploys proactive threat mitigation strategies, enabling you to stay one step ahead of attackers and efficiently prioritize vulnerabilities for mitigation. With features such as Sigma Scheduled Hunts and IOCs & YARA Scanner, our scalable cloud-delivered solution is capable of meeting different business needs.

We also provide personalized 24/7 local support, empowering your organization to take control of its cybersecurity and fortify its digital defenses effectively.

CONTACT US NOW TO DISCUSS YOUR SECURITY REQUIREMENTS AND START PROTECTING YOUR SME AGAINST LOOMING CYBER THREATS.

CONTACT US NOW