OTAVA

SECURE & COMPLIANT MULTI-CLOUD SOLUTIONS

S.E.C.U.R.E.™ Framework

Decoding the Complexity of Cybersecurity

- **Common Cybersecurity Misconceptions Addressed:** The document debunks common cybersecurity myths, including the adequacy of basic cybersecurity protection, the misconception that cyber threats do not target medium and small businesses, and the belief that regulatory compliance equals complete security.
- **A Layered Approach to Cybersecurity Doesn't Have to be Complex:** The S.E.C.U.R.E.™ Framework provides a multi-component strategy to assess your current security posture, identify gaps, and offer alternative strategies to refine and improve your overall security.
- **Customized Implementation:** Recognizing the unique needs of each business, the S.E.C.U.R.E.™ Framework offers flexibility in its application. Companies are encouraged to prioritize and implement their components based on their specific security requirements and business objectives.
- **Continuous Improvement and Adaptation:** Cybersecurity isn't a set-it-and-forget-it deal. The S.E.C.U.R.E.™ Framework advocates constant evaluation and refinement to adapt to new cyber threats. This proactive approach ensures businesses are prepared to anticipate and mitigate cyber-attacks rather than just reacting to them.

Today's Problem

The saying "better safe than sorry" is essential to remember, particularly when it comes to cybersecurity. No one wants their business compromised because bringing things back to their initial state is expensive and hard. Even if you have the best security measures in place, it's important to remember that cyber threats are quickly evolving and becoming more sophisticated, and at times, it may feel impossible to stay current with your cybersecurity strategies. Therefore, the best way to safeguard your business assets is by detecting threats early or intercepting them as soon as possible.

We understand cybersecurity can be overwhelming and complex, especially if you don't know where to start. This tech brief will provide you with a framework that can serve as a guide to help you strengthen your security posture. By making incremental improvements over time, businesses can implement a layered defensive and recovery strategy to safeguard their data, reputation, and profitability.

Contents

Common Misconceptions about Cybersecurity

Before we get into it, let's discuss a few common misconceptions about cybersecurity:

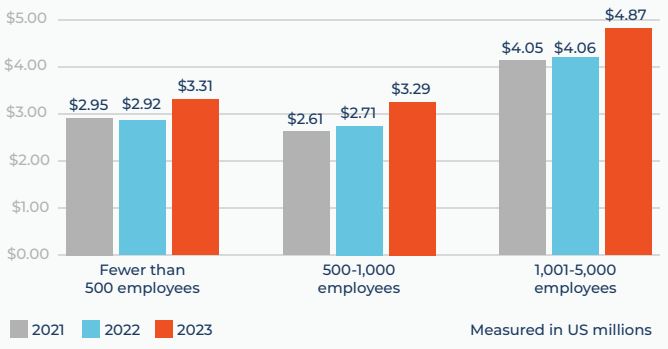
1. **Our business is well-protected since we have installed both firewall and antivirus software.**

   Antivirus software and firewalls are essential components of cybersecurity. However, more is needed to protect small and medium-sized businesses from modern cyber threats. Modern cyber threats are sophisticated and can bypass traditional antivirus solutions; that alone is insufficient to keep businesses safe. A layered approach is necessary to achieve comprehensive security, including solutions such as firewalls, intrusion detection systems, and regular security audits.

2. **We are too small to be a target, and our data is not valuable to hackers.**

   This is just not true. The reality is that small and medium-sized businesses are often more appealing to attackers due to their typically lower levels of security, despite many businesses believing that cybercriminals only target large corporations or government entities. In 2023, smaller organizations faced considerably higher data breach costs compared to the previous year. (See Figure 1.1)

Cost of a Data Breach By Head Count[1] *Figure 1.1*



[1] *IBM, "The Cost of a Data Breach Report 2023," 2023. [Online]. Available: https://www.ibm.com/reports/data-breach*

3. **Compliance = Security**

   Many believe that meeting regulatory compliance standards, such as **HIPAA**, **SOC** (Security Operations Center), **PCI**, or others, is enough to ensure a comprehensive security posture. However, this is a common misconception. In reality, compliance only represents the basic requirements for security. The best security practices go beyond these regulatory compliance mandates. Compliance should be seen as the starting point of your journey rather than the end goal. That being said, partnering with a company that prioritizes both compliance and security is a great way to start.

S.E.C.U.R.E.™ Framework - Layered Defense and Response

Imagine that your business is your home and that robbers are trying to break in. You wouldn't just lock the front door and forget about it.

Instead, you would check to ensure all the windows are closed and all other entry points are locked. You might even have a guard dog, an alarm system, a few cameras, and plans in place in case the robbers try to break in. That's essentially what the S.E.C.U.R.E.™ Framework does - it helps keep your business safe from digital robbers.

Elevate Your Security Posture

When it comes to security resilience, we believe in preparing you for what's next and ensuring you're protected every step of the way. Cybersecurity is not a 'set it and forget it' matter. This requires a commitment to update and refine your security measures regularly. It involves ongoing processes and practices to protect systems, networks, and programs from digital attacks.

OTAVA'S S.E.C.U.R.E.™ Framework is built on an acronym but most importantly it's an approach to think strategically about business continuity and the importance of layering preventive measures, visibility, contingency plans, and constant improvement to meet businesses where they are on their path to being secure.

The S.E.C.U.R.E.™ Framework acts as a blueprint to build a solution tailored to your specific needs, designed to isolate different components based on your business priorities, ensuring that you can protect your business from potential cyber threats. With this framework, you can keep your virtual doors locked tight and your walls sturdy against any online storm, safeguarding your organization against potential cyber threats.

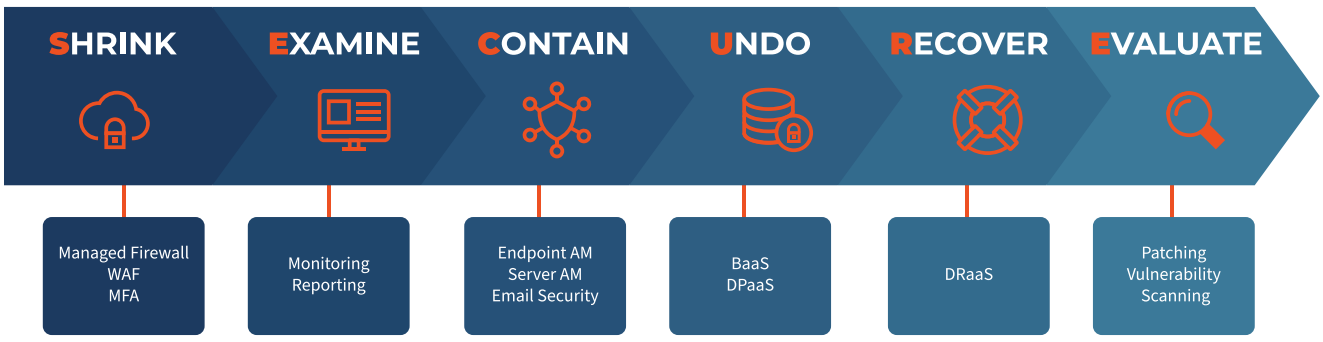
This approach to cybersecurity ensures that your defenses are comprehensive and ingrained in the fabric of your business operations. It's a continuous journey of improvement, where the goal is not just to respond to incidents but to anticipate and mitigate them before they can take root.

With the S.E.C.U.R.E.™ Framework, your business is not just reacting to threats but actively engaging in a continuous cycle of defense and refinement.

So, what does S.E.C.U.R.E.™ stand for?

- **Shrink:** the **attack surface** and protect access points
- **Examine: monitor and analyze** anomalies and event threats
- **Contain:** the **attack vectors** to reduce the proliferation of any attack
- **Undo:** take action to **isolate and restore** infected data
- **Recover:** to achieve **business continuity** of operations
- **Evaluate:** continual improvement of your **security posture**

Figure 2.1



Shrink: Minimizing Exposure, Maximizing Security

Explore strategies to shrink your organization's **attack surface** and strengthen access controls, making it harder for attackers to find and exploit vulnerabilities. It also ensures that your resources are not stretched too thin by minimizing the number of entry points.

- Identifying and eliminating unused or unsafe services and protocols.
- Implementing strict access control measures and privilege restrictions.
- Regularly update and patch systems to close off known vulnerabilities.

Potential Solutions

Managed Firewall

Web Application Firewall

Multi-Factor Authentication

Things to Consider

- Do you have a game plan if your firewall goes down?
- Are you currently leveraging MFA anywhere in your environment?
- How are you reducing your attack surface today?
- What happens when credentials are compromised?
- Are all employee devices connected into a secure infrastructure itself?

Examine: Vigilance Through Visibility

Understand the importance of continuously **monitoring and analyzing** system anomalies to detect potential threats before they escalate. It is crucial to know how to identify unusual behavior to make this strategy effective. You can achieve this by either hiring qualified professionals to manage and examine your environment or by providing training and education to your resources so that they can identify and report such behavior.

- Setting up comprehensive monitoring systems for real-time threat detection.
- Conducting regular system audits and behavior analytics to spot irregularities.
- Training teams to recognize and respond to the signs of a cyber intrusion.

Potential Solutions

Managed Monitoring

Reporting

Things to Consider

- Do you have any security reporting in place to assess your security posture?
- Do you have any pain points regarding security that you wish you had better understanding and transparency?

Contain: Halting the Spread of Cyber Threats

Focus on containment strategies to **contain the attack vectors** across networks and devices, minimizing damage and maintaining core functions.

- Isolating affected systems to prevent lateral movement of attackers.
- Implementing automated response measures to quickly address breaches.
- Establishing communication protocols to manage information during an attack.

Potential Solutions

Server Anti-Malware

Endpoint Anti-Malware

Email Security

Things to Consider

- Do you have any anti-malware or antivirus software installed on your endpoints, and are you utilizing all of the endpoint software's features?

Undo: Rapid Response and Data Restoration

Learn the importance of having a robust incident response plan and effective data backup strategies to quickly recover from cyber incidents by **isolating and restoring** infected data.

- Preparing and regularly testing incident response plans.
- Utilizing S.E.C.U.R.E.™, encrypted backups and ensuring they are up to date.
- Practicing data restoration processes to ensure minimal downtime.

Potential Solutions

Managed Servers

Backup & Data Protection

Did you know?

93%

of companies that lost their data for 10 days or more filed bankruptcy within one year of the disaster.[2]

[2] *S. Bennett, "Disaster Recovery Statistics 2024 – Everything You Need to Know," 2024. [Online]. Available: https://webinarcare.com/best-disaster-recovery-software/disaster-recovery-statistics/#6.*

Recover: Ensuring Operational Continuity

Having a business continuity plan and disaster recovery to maintain operations during and after a cyber incident.

- Designing and implementing a business continuity plan tailored to your business.
- Training staff in emergency procedures and roles during recovery operations.
- Regularly test and update business continuity plans to handle evolving cyber scenarios.

Potential Solutions

Disaster Recovery

Do you have a data disaster recovery plan?

46%

of organizations don't have a disaster recovery plan in place.[3]

[3] iland & Zerto, "When Plan B Goes Wrong: Avoiding the Pitfalls of DRaaS," Incisive Media, 2021

Evaluate: Continuous Improvement for Cyber Resilience

Understand the ongoing process of reviewing and improving security posture, learning from incidents, and adapting to new threats. Evaluation is a continuous process where you assess and improve security measures. As the threat landscape changes, so too must defenses.

- Conducting post-incident analyses to identify lessons learned and areas for improvement.
- Staying abreast of new cybersecurity trends and technologies.
- Engaging in regular security assessments and updating the S.E.C.U.R.E.™ Framework accordingly.
- Scanning your environment for emerging vulnerabilities on a regular basis.

Things to Consider

- Do you regularly assess your security posture?
- Have you recently gone through any compliance audits?

Potential Solutions

Vulnerability Scanning

Managed Patching

Final Thoughts

Having a well-planned and structured approach towards cybersecurity is extremely important, as not doing so can lead to failure. The S.E.C.U.R.E.™ Framework is more than just an acronym, it represents the essential multiple components that one needs to adopt in order to safeguard against constantly changing cyber threats.

The framework includes multiple components, but you do not have to implement all of them at once. Instead, you can isolate the components based on your business priorities. The framework involves:

- Reducing the attack surface of your digital footprint **(Shrink)**.
- Constantly monitor and analyze your environment to identify unusual activities that could indicate a breach **(Examine)**.
- Limiting the reach of any successful attack **(Contain)**.
- Quickly mitigating any impact by isolating and reversing the damage **(Undo)**.
- Restoring your systems to operational status with minimal downtime **(Recover)**.
- Continually refining your security measures through vulnerability scanning, regular business continuity plan reviews and updates **(Evaluate)**.

The S.E.C.U.R.E.™ Framework builds up your cybersecurity bit by bit. It's all about layering up and keeping at it. Incorporating OTAVA's S.E.C.U.R.E.™ Framework into your business will create or strengthen your business continuity plan.

Securing your business from cyber threats can seem like a big task, but it doesn't have to be! It's all about having the peace of mind that comes from knowing your business is S.E.C.U.R.E.™ so that you can focus on growth and success. Partnering with the right experts may be the easiest way to achieve comprehensive and ongoing protection so your security is always in great shape.

With OTAVA's S.E.C.U.R.E.™ Framework, your business isn't just surviving - it's thriving securely.

Learn More

OTAVA solves modern, critical challenges for their customers via sophisticated secure and compliant multi-cloud solutions aligned with industry standards and people-centered, best-in-class professional services built on the foundation of collaborative relationships.

When it comes to implementing cloud solutions, OTAVA knows one size doesn't fit all, so its team of IT professionals will help you along your journey to migrate and integrate your cloud solutions in adherence to the S.E.C.U.R.E.™ Framework.

Contact an OTAVA expert today to learn more by visiting otava.com/secure.

OTAVA®

SECURE & COMPLIANT MULTI-CLOUD SOLUTIONS