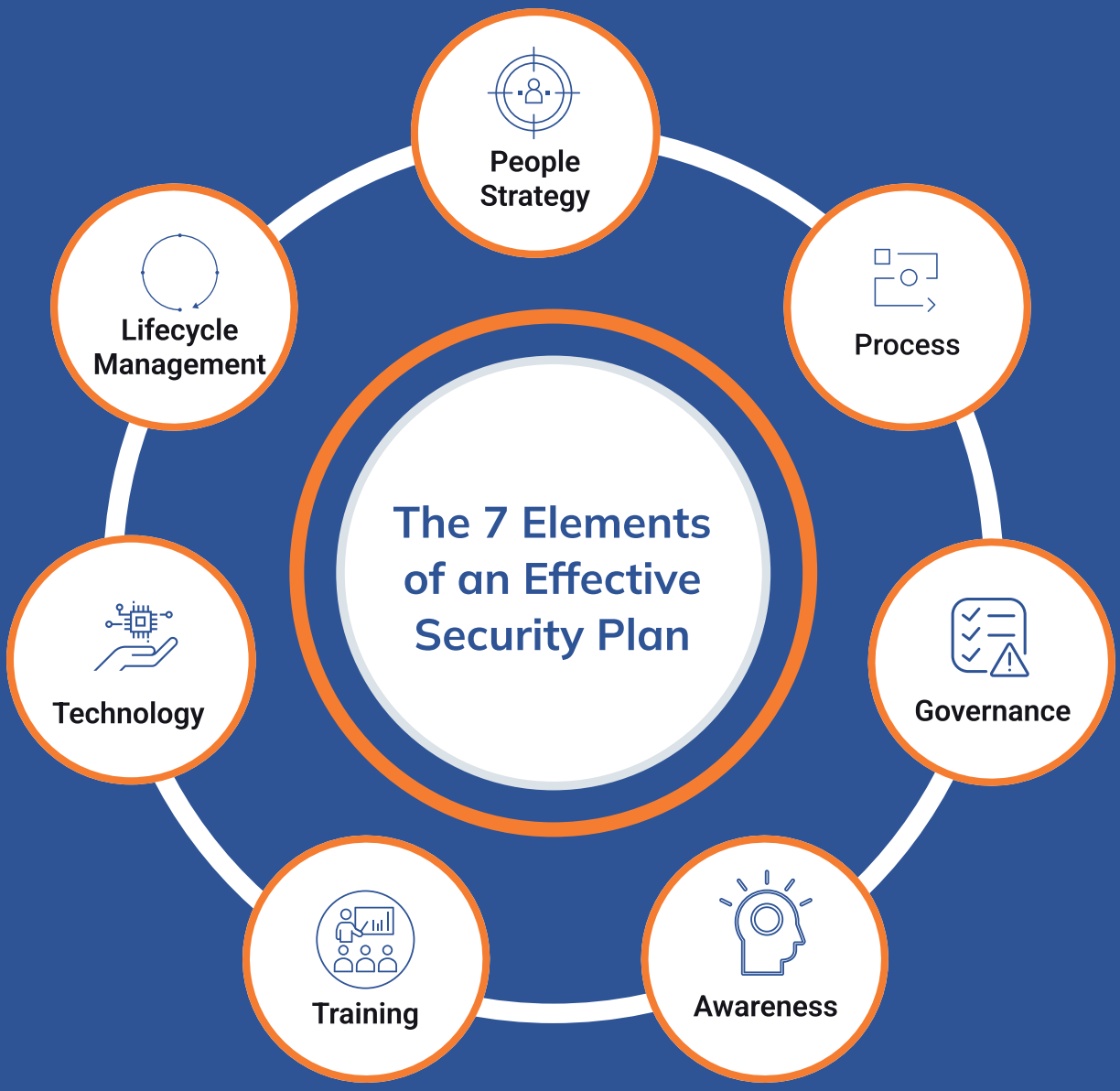
The 7 Elements of an Effective Security Plan



Atriade

www.atriade.com

Contents

Introduction

While every security plan will have its own nuances, given the unique details and challenges found at different organizations, our extensive experience in the security field has led us to the conclusion that any good security plan must have seven elements: people strategy, process, governance, awareness, training, technology and lifecycle management.

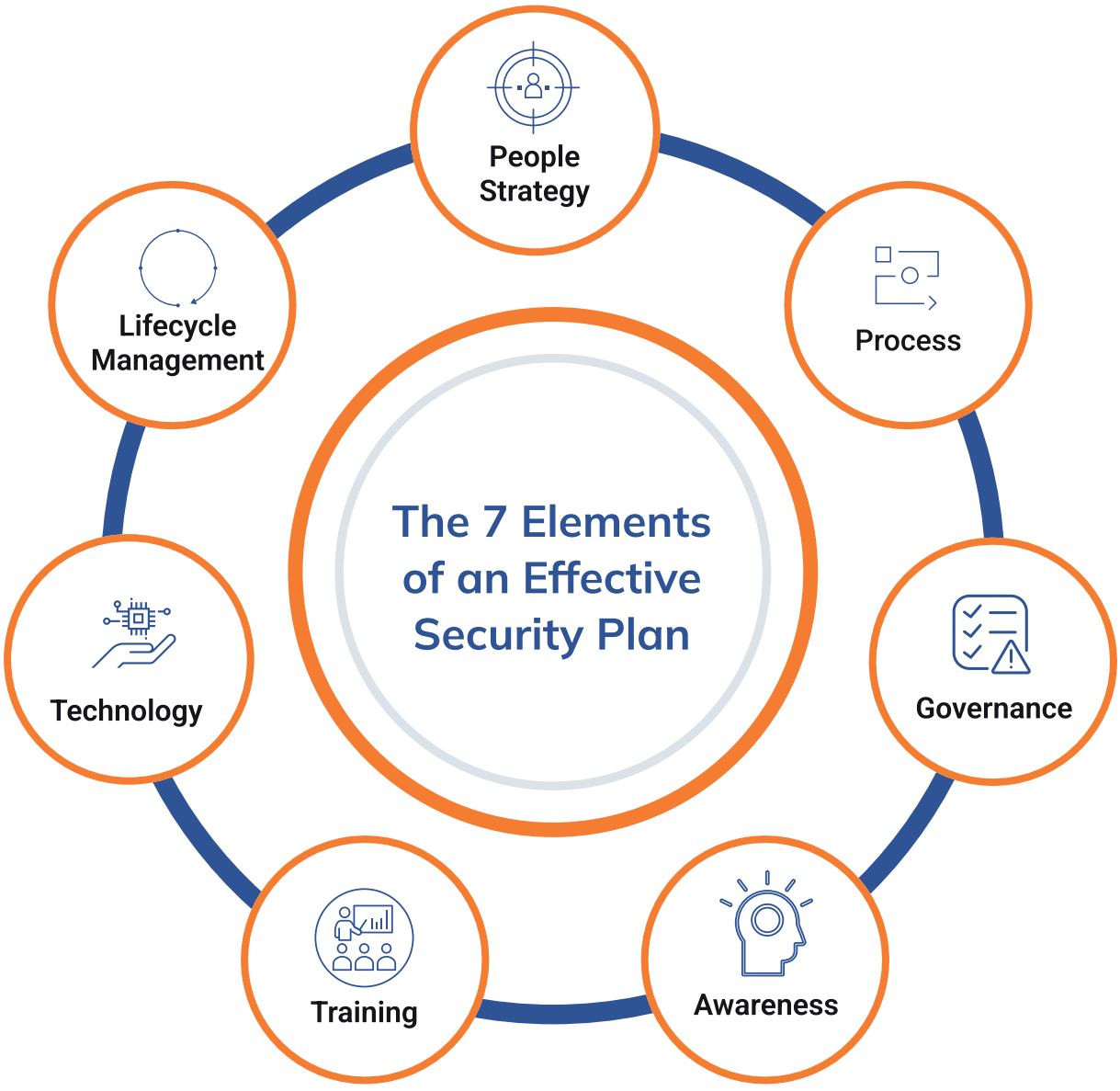
Before moving into specifics, let's start with some overarching thoughts about security plans in general.

All organizations, no matter what size, will benefit from having a cohesive, forward-looking security plan. In our experience, however, we find many plans are not up-to-date or practical, and they have been siloed, meaning there is not actually an orchestrated plan in place.

It's rare for organizations to have all seven pieces of a good plan in place — most times there are gaps — and often the plan goals are misaligned.

For example, mitigating risk should be at the core of any security plan, rather than focusing on any one element, such as installing cameras.

In the follow pages we will define the seven key elements an effective physical security plan should contain.


People Strategy
Process
Governance
Awareness
Training
Technology
Lifecycle Management
The 7 Elements of an Effective Security Plan

01 People Strategy

When we say, “people strategy,” we mean two things: a plan for onboarding, growth and offboarding as well as a staffing model that includes requirements and resources. We commonly find organizations do not have data to indicate what staffing levels they need, and they lack workload calculations to inform decision-making.

A data-driven staffing model is an excellent tool to drive people-focused decisions, since it will forecast operations, measure workloads in time (frequency x resolution time) and identify capacity in time by resources. To create this model, the data needed includes a task inventory — frequency of task, task resolution time and resource impact of task — and the capacity of resources — administrative and human time.

The organized data collection process required for this effort has three stages

Define your scope

- Ensure you're gathering valuable data points that are relevant to your business
- Define measurements carefully and clearly to get useful metrics
- Identify and/or develop quality data sources that can be leveraged as needed in the future
- Use segments to simplify your analysis and avoiding flawed correlations

Develop an accurate task inventory

- Task data — criticality, resources impacted, systems used
- Time to resolve each task
- Frequency of each task over time

Collect data

- Establish a consistent timeframe to gather task frequency
- Conduct time trials and capture challenges
- Build data collection into operations to make it part of the team's culture
- Use all available data sources and make sure they are valid

We have gained many insights from seeing this process roll out, starting with the importance of starting small and evolving while standardizing data collection. And when it comes to workload measurements, we suggest taking the time to collect large enough data sets to provide more accurate mean values and identify outliers that may potentially skew your results.

Beware of capacity traps!

When trying to calculate human capacity, remember that an eight hour workday does not equal eight hours of capacity. You need to account for several possibilities including lunch, breaks, meetings, email and think time. People are not machines moving uninterrupted from task to task and will never provide a full eight hours of capacity.

We also recommend using external resources to assist with the modeling process, as that objectivity can be invaluable, and focusing on holistic solutions to issues that arise in the areas of process and technology.

02 Process

Process is defined as a series of operations to achieve a desired goal in a consistent fashion. A good process requires structured and holistic thinking, as well as an objective, resources, actions and timing.

We commonly find organizations have processes that are not well defined, and they are often not helpful to the people who need them. It is critical to develop a formalized process management plan, so the right people get the right information when it is needed.

While every organization is different, we often recommend that process be approached in two ways: Process Planning and Process Delivery.

Process Planning

Process planning has four elements: inventory, assessment, change management and feedback. These four elements help take a holistic approach at process planning.

- Inventory involves category, process data, priority/criticality, timing and form. Having a clear picture of your processes helps you understand their value and measure their impact. It also helps keep a review cadence and prioritize process needs.

- To ensure the security process is continually improved upon, a formalized assessment strategy should be implemented. This strategy should include evaluating all elements of a process from value to performance. Value tests should determine whether the process aligns with the mission, mitigates risk or adds value. Performance tests should consider functional success, support by stakeholders, as well as what kind of feedback it generates. Those deemed to be failing can be updated with new steps, retired as legacy processes or transferred to another team.

- Managing change is critical to operational success. Business requirements and risks change over time and the security operation and process needs to align accordingly. The change management process should not be limited to technologies. Changes made to process should be carefully considered. Organizations should formalize this effort and consider process onboarding and offboarding, approvers and approvals.

- The people who utilize your processes will understand them best. Particularly where they succeed and fail. Often your best sources of information aren't involved in strategy meetings, so it's important to develop an effective feedback process. Create a feedback strategy and mechanism that is transparent and inclusive. In cases where anonymity is preferred, allow that as an option.

Process Delivery

Process delivery should be focused on delivering the right content to the people who need it at the time they need it. The content delivery ecosystem should be easy to use and we recommend considering three areas of focus:

Categorize Information

- Create and categorize information into layered content to ensure it is delivered to the right audience.
- Strategic and tactical information should be available to leadership and managers who are leading or driving the organization.
- Task data should be made available to the users conducting day to day operations.
- Division of content can help create “need to know” channels and also ensure that people see what they need to see and are not overwhelmed by information that isn’t relevant to them.

Content Management Process

- Develop an organized content management process to maintain accuracy and consistent access of information.
- Creating a single, consistent source of processes limits search time.
- Developing policy for version control to ensure no rogue versions of process or documentation circulates is important for consistency of information.

Appropriate Tools

- Utilize appropriate process tools to deliver data quickly and efficiently.
- Prior to tool selection, ensure you complete a comprehensive requirement gathering exercise to ensure that the technology you select works for all team members.
- Focus on creating a good user experience to limit workarounds generated by inconvenience or poor access control.
- Make sure any technology you select is appropriate to your team's skillset to ensure they can use it effectively.

Ultimately, process should be well planned and delivered in a way that aligns with the organization's requirements and culture.

Creating a formalized process strategy that accounts for proper planning, assessment, change management and an effective delivery will result in a flexible and efficient execution.

03

Governance

Having the right people and processes in place is a good start, but without proper governance, things can go awry.

We commonly find issues involving poor or non-existent collaboration, a vague understanding of who does what and the lack of a unified message.

The focus of governance should be transforming siloed groups into a collaborative organization, clearly documenting roles and responsibilities and using communications best practices.

Also important are defining security's seat in the C-Suite and implementing role-appropriate task management.

Steps to build good governance include cross functional collaboration across various departments and stakeholders; steering committees to discuss multi-disciplined goals and objectives, vertically aligned organizational structure to provide uniform communication and escalation means.

Organized Program

- Creating an organized and strategic program to share information across disciplines helps align organizational priorities, reduce redundant efforts, collaborate on projects jointly. It builds the necessary trust to execute operations and projects efficiently.

Steering Committees

- Steering committees add a layer of executive buy-in and drive long term objectives. They provide the security management organization an opportunity to build strategic programs with proactive executive adoption and sponsorship.
- Steering committees can also help the security leadership to be in tuned with the organization's objectives.

Vertical Alignment

- Vertically aligned organizations are important in developing a uniform set of policies, communication and escalation procedures.
- Once combined with cross functional collaboration and steering committee structure, a properly vertically aligned security organization can really achieve effective and efficient means to share information, transfer knowledge and resolve issues.

04

Awareness

With respect to a good security plan, awareness involves having an aligned culture, formal process, smart content and regular outreach. At its core, it provides a blueprint on how to behave in emergency and non-emergency situations.

Formalizing an awareness plan consists of identifying your target audience, behavior types, messaging and timing. It's especially important to know your audience, so you are communicating in a way that will make sense and resonate with them.

Awareness Considerations

Other aspects of awareness are:

- Engaging with users
- Developing partnerships
- Recruiting executive sponsors
- Determining content delivery via traditional channels, through digital and social media, and even signage

Your all-encompassing goal should be to establish a culture of safety, not surveillance. A negative sentiment can make it difficult to develop relationships and establish and maintain partnerships.

Getting buy-in from leadership is extremely important to help gain consensus and adoption.

05 Training

Any security plan will experience challenges if team members haven't been appropriately trained in what their roles are with respect to organizational safety. When training does take place, it often isn't done with a lot of specificity, and that is a mistake.

It's critical to customize all trainings to the specific audience, since not all risks apply to everyone.

User Engagement

From a user engagement perspective, you'll be best served by employing a variety of training channels, such as:

- Town halls
- Social and digital media
- Newsletters
- Social events

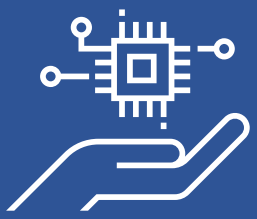
Using a mix of traditional and modern tools—apps, messages and notifications, and events and programs—ensures your training efforts will reach all audience members. It's also invaluable to create a feedback and refresh loop, to gather insight and ensure safety-related information is available on an ongoing basis.

While technology has its advantages, especially in a distributed workforce, some trainings still must be conducted in person. This is the case with fire evacuation and other types of life safety training, including workplace violence and first aider training.

These situations require a person to be able to clearly navigate different elements in their environment and to potentially help others during high-stress situations.

Ensuring that team members are present to participate in these types of trainings are critical to emergency response.

06



Technology

The biggest issue when it comes to technology in a security plan is how to choose and deploy the right system.

Shopping without clearly defined requirements can result in purchases being made that are not necessarily aligned with specific needs.

To avoid making an unfortunate—and likely expensive mistake, your journey to a technology purchase should begin by understanding your current state and developing your functional requirements.

You want to ensure you leverage existing systems and parallel efforts, and align your goals with business and technical roadmaps. It's important to understand market trends and eliminate noise as you evaluate and validate new technologies as well as establish a short- and long-term roadmap.

Leverage Your Lifecycle

Some questions to ask yourself along the way include:

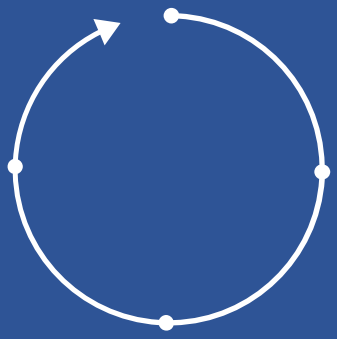
- What are my risks?
- Can my existing portfolio mitigate these risks?
- What is my risk tolerance?
- What are my peers doing?
- Will it work in my environment?
- How do I responsibly deploy it?

Rather than getting overwhelmed by the bells and whistles available, it's invaluable to make a data-driven business case based on actual incidents. Once you have that deep knowledge in hand, you'll be able to choose technology with surgical placement in mind. Metrics always resonate.

Technology trends to watch for include consumer trends like mobile, cloud, frictionless, health and wellness, and identity and access management, truth about privacy, and user experience.

Once you have made your decisions, an informed five-year deployment plan that consists of technology elements, costs and a specific rollout schedule will be critical to your success moving forward.

07 Lifecycle Management



Atriade conducted a poll on LinkedIn asking: “What Lifecycle Management Process Do You Use?” Because the management of the security technology lifecycle poses a substantial challenge for many organizations, we wanted to understand how they were approaching the process itself. We see this gap causing budgeting challenges and difficulties in making business cases for upgrades.

The results of our poll reinforced our understanding of the current marketplace for security technology lifecycle management. A majority of respondents (65%) are using a formalized tool, but a significant portion of the marketplace (35%) are using a manual process or have nothing at all.

Perhaps the rarest component of a good security plan is lifecycle management. If it's done at all, it's usually done poorly; current practices often use an Excel spreadsheet and rely solely on discoverable assets. Given the significant investment made in security technology, it is surprising how many organizations experience challenges in this area, when a small investment of $20,000–$30,000 would ensure forward-thinking data is available.

An in-depth lifecycle plan has three components:

Importance

- Mission-critical
- Awareness of current state
- Proactive planning of future state
- Funding and administrative roadmap

Elements

- Technology
- Maintenance
- Useful life of technology
- Licenses
- Policies
- Funding pipeline

Future State

- Facilities management
- Inventory management

To provide a simplistic example of necessary future thinking, if you plan to replace your technology every five years, and it takes one year to get funding, the actual lifecycle of your equipment is four years. Asset management is a built-in cost of doing business, and in an area like security, where falling behind can inherently be unsafe for the organization, it's well worth investing in.

Key Takeaways

Having the right plan in place will do more than reduce risk; it will bring an organization closer together, working toward a common goal.

People Strategy

- Develop a clearly defined strategy for staffing that takes into consideration not just skillsets but a balanced, measured workload to ensure resources are utilized efficiently.

Process

- Create a process ecosystem that delivers the right information to the right people when they need it. Change management for process should be well designed and properly implemented.

Governance

- Use governance models to transform siloed groups into collaborative teams. Develop clear communication paths and create value to be shared across the organization.

Awareness

- Develop an awareness model that leverages directed content and regular outreach to create a culture of safety and security.

Training

- Create useful training that empowers employees and is tailored to the audience to help improve performance metrics.

Technology

- Invest the time to clearly define requirements and develop a clear plan for deployment that considers risk and is appropriate to the culture of the organization. Deploy technology responsibly.

Lifecycle Management

- Create an operationalizable lifecycle management plan to help keep technologies secure and provides budget forecasting to maximize value to the organization.

Additional Reading

Understanding Insider Threats and Mitigation Techniques

Best Practices around Security through Environmental Design

Designing and Building an Effective SOC That Meets Your Unique Needs

How To Get Camera Coverage Right

How To Construct a Well-Written RFI to Make Informed Decisions

How To Effectively Use a Proof of Concept

Are You Managing Your Asset's Lifecycle Effectively?

Replay of Webinar: The 7 Key Elements to Build an Effective Physical Security Plan

About Atriade

Atriade has best in class expertise in system designs, policy development and training exercises for corporate office space.

Our team intimately understands identity and access management, visitor access, incident management, traffic flow and overall risk profile of end user environments. Our solutions are always risk focused to achieve the right value add for your business operations.

We are heavily engaged within the security and facilities industries. This allows our SMEs to properly vet technologies and solutions offered by manufacturers. We ensure that they indeed accomplish what's promised and more importantly, meet your specific requirements.

We conduct product testing, review cyber security requirements and coordinate infrastructure needs before any large-scale implementation.

Atraide has an engaged and informed approach with our customers. Our unbiased and independent client advocacy ensures a risk mitigation focused solution for your operation.

Learn More About How Atriade Can Help Mitigate Your Security Risks

Visit our website for more insights

Follow our Company page

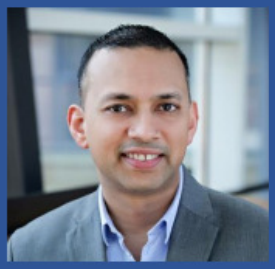
Contact us: 201 721 8570

Subscribe to our LinkedIn Newsletter: Take A Risk

Connect with us on LinkedIn:

Reese Huebsch - CERT Insider Threat Certified

Mohammed Atif Shehzad



Saif Nomani