A Recipe for Resilience

DR. MIKE LLOYD
CHIEF TECHNOLOGY OFFICER

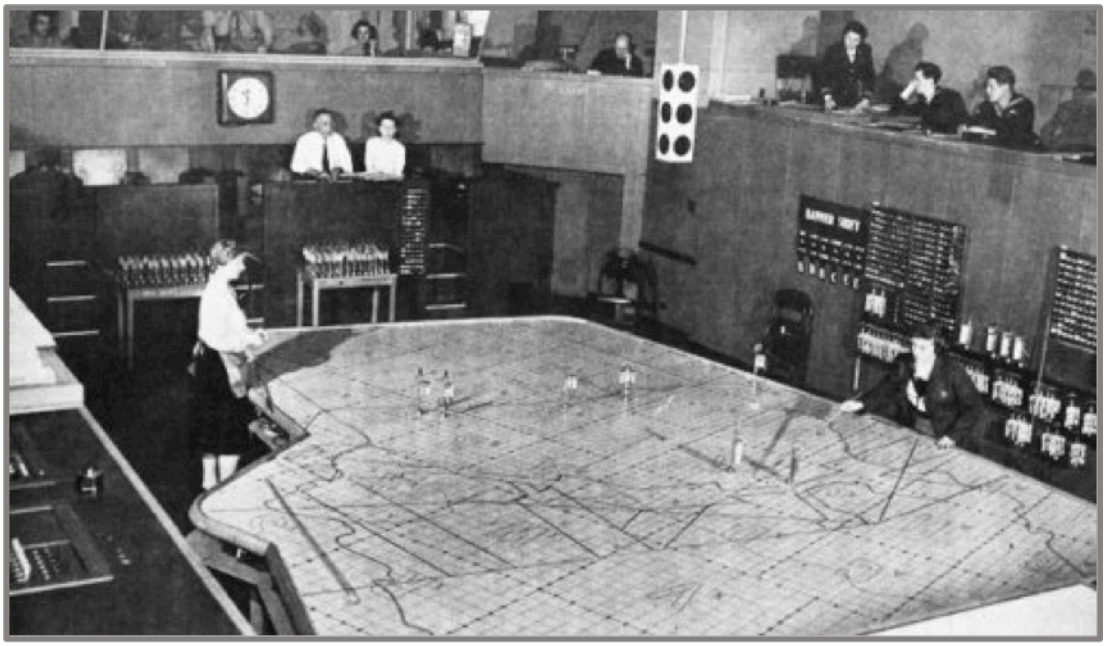
The goal lines in security have shifted. Perfect protection is widely recognized as unobtainable. Breaches are inevitable—it's how you handle them that matters. These days, resilience is the goal. Boards have moved from "just tell me we're safe," through "show me a risk assessment to prove you're paying attention to business context," all the way to "demonstrate our resilience for public filings."

This new focus on resilience requires a shift in thinking—away from trying to block everything towards understanding how to bounce back. Despite the recognition that even very sophisticated defenses can be breached, this is a pragmatic, not a defeatist approach. It is used by military thinkers, who develop strategies to compensate for damage to their forces or territory.

I find forward-thinking security teams welcome this change in approach, but often lack a clear, guiding model for how to build up a resilient organization. It's a broad challenge, covering every aspect of people, process, and technology. This document aims to provide a framework that can guide your approach, in your specific organization.

Building a Security War Room

The technical challenges we face are new, but the situation is not. Modern security teams are not the first to face personnel shortages while being attacked by dedicated, persistent and well-resourced adversaries in a world of changing technology. This picture shows us one historical example.



This is a war room bunker in London, during the Second World War. The picture may be grainy, but there are several important lessons that come from understanding what is happening in this room. It offers a powerful model of resilience—showing what it takes to succeed in a defensive war, when seriously outgunned and dealing with significant shortages.

Looking at the war room picture, we can see a basic three-part layout of the room—the upper galleries, the lower map table, and the middle layer.

In the upper galleries there are people processing data from the outside world. Think of it as real-world sensor data. It is essential to decision making, but there is a lot of data from all reporting sources. Some of the source technologies are new—in this example, radar. Each new sensor technology requires detailed understanding about what can and can't be detected and the risk of false positives or ambiguous signals. All this incoming data must be cleaned up, compared, reconciled, and eventually conveyed down to the map.

The lower map table is where all this processed information from different sources is combined. The team has defensive information about where forces are arrayed, where they are moving to, and where the gaps in coverage are. There is also the murkier

information about the enemy and its movements. And all this happens on varying terrain. Military thinkers agree that these are the three necessary types of data—terrain mapping (to understand the ground you're fighting on), force accounting (keeping track of your own assets), and enemy intelligence (which comes with significant fog of war).

Once you have terrain, defense and attacker information, it makes the most sense to present them visually. In the photo, there's a gentleman wearing a tie who has what is known as situational awareness. From his vantage point, he can see the situation, draw conclusions, and allocate resources to the oncoming fight. Rooms like this were frequently used to present information to higher level decision makers, so they could see highly complex and disparate information feeds condensed into a digestible, comprehensible picture of the situation.

Taking the Long View

Today's security leaders and architects are addressing challenges much like these. The first step is to realize the nature of the war we're fighting. Attackers are using automation, continually probing our defenses. Some attackers don't even care who you are—they are just sending out robots to hunt for easy victims. Others are patiently stalking your specific organization, using lures and watering holes to gain an entry point. Even if you win a great victory against one adversary today, there will be a new one tomorrow using a new kind of evasion or deception. We have to take the long view—planning for survival, not for victory. This means we must increase the costs for attackers and reduce our costs to recover. In a word, we need resilience.

Building Resilience

Achieving digital resilience consists of three primary objectives, focused on increasing the costs for attackers and decreasing the cost of defense. In order, these objectives concern what you need to plan for before, during, and after an attack. They are:

- Be hard to hit
- Detect immediately
- Recover rapidly

These high-level goals can be broken down into a series of ten practical steps:

1. Gather inventory (network and endpoints)
2. Build a map of your whole infrastructure (cloud and physical)
3. Investigate "dark space"—parts of your organization that are not mapped
4. Identify the most critical parts of your organization on your map
5. Integrate more data feeds from diverse data sources
6. Harden individual endpoints by following standardized best practices
7. Establish zone-based defenses to segment parts of your operation
8. Document access expected to cross major zone boundaries
9. Detect anomalies, and open investigations as they arise
10. Fold lessons from investigations back into improved architecture and segmentation

These steps can be run sequentially, as distinct initiatives, building towards a goal of a mature process. Each step produces value of its own, and by the end (step 10), organizations can loop back to stage 5, improving and refining their knowledge and control of the infrastructure.

RedSeal's software is designed as a platform for these steps, serving as the table in the World War II war room. RedSeal provides both a map and a single source of truth, integrating distinct data silos about networks, endpoints, vulnerabilities and your virtual and physical equipment. The inventory and map greatly reduce the labor in setting up steps 1 through 8 of the recipe for resilience, and act as a launch point for specialized incident response and investigation teams. Steps 9 and 10 are generally not automated, since humans are the best equipped to deal with the highest-level analysis—the psychology, strategy, and objectives of the adversaries of your particular organization.

SOME CONSIDERATIONS

Don't Aim to Show Everything

The people who designed the London war room understood one of the great lessons from cartography—the art is in what you leave out. Technical people often struggle with this point—we can tend to equate precise detail with usefulness. Anyone who makes maps can tell you this is not true. After all, a 1:1 scale map isn't useful or practical. You can't represent a battlefield in full detail on anything smaller than that battlefield. The

real art to situational awareness is deciding which details can be left out so the big picture becomes clear. We want decision makers to see the forest, not the trees (or worse yet, every detail of the bark).

The war room works because an overwhelming mass of tactical data is reduced to the essential factors for effective decision making. It turns what could be a chaotic mess into strategic insight. This is the challenge most security teams face today—too many facts, not enough context, and precious little insight or situational awareness.

The Role of Prioritization

Security teams are forced to prioritize. There simply aren't enough hours in the day or enough trained security professionals for any other starting point. We'd like to block every threat and avoid every kind of damage, but that isn't possible. Much like British defenders in World War II, we are outgunned and out staffed by adversaries with superior weaponry. But as they showed, resilience, prioritization, and optimization can overcome enormous challenges. We can optimize our defenses ahead of an attack, detect rapidly, and respond effectively when the breaches occur.

Prioritization starts by understanding and mapping your business, starting from the most critical assets. Ideally, we'd have a complete inventory or a complete map, but capturing full information is never easy. In most organizations, a complete map of every asset remains an elusive goal—a good target to strive towards, but not something you can build as your first stage. Rather, the first stage is to start from the business—what are your organization's goals, how does the organization function? Which parts of the infrastructure are the most critical to your business?

In a physical war, critical assets are well known, highly localized, and well mapped. This is not the case in most organizations. Critical business functions often depend on poorly-understood infrastructure, due to loss of tribal knowledge or just poor recording of changes. The goal at this stage is to understand business priorities, identifying which mission objectives are truly critical. But mapping these business priorities down to individual assets can be a serious challenge.

To address it, you need a degree of active discovery. You try to identify each asset, then establish what it's for and determine if it's a business priority to protect it. Therefore, a good first technical component of your war room is an endpoint discovery technology—a vulnerability scanner or an endpoint management system. While these systems can't generally provide deep insight into business purpose of the assets that they find, or even who is responsible for them, they provide a place to start.

In practice, then, the first two areas of focus should be: 1) a description of the business and its operation, prioritized at a high level, and 2) an asset inventory at a low level. The chasm between these two is the first area to bridge—which assets are for what? Identifying the role and criticality of assets can be tedious, but it will prioritize your attention and keep your war room from being awash in details.

Combining and Cleaning Data Feeds

One major problem in real-world war rooms is incompleteness of data—the "fog of war." Contemporary security technologies face similar issues, despite what vendors sometimes tell you. Each technology we deploy can only see the technical aspect of the problem it focuses on. There is no automatic means to discover the business role or mission priority of a given asset. That said, we can find clues if we look intelligently. For example, devices found in high availability pairs or load balanced server farms are more likely to be important, since the business is spending money to ensure uptime.

One effective technique to improve your data is to use feeds to strengthen and improve each other. Every source of data about your organization has a somewhat different view—due to either different focuses or from deployments done by different people at different times.

These differences may sound like a problem, but they can actually be a great help when your goal is to be digitally resilient. Security teams need as complete a picture as possible to locate any blind spots. Most other teams can get by with data covering just their most important focus areas. But the places not being actively managed and cleaned up are exactly the places the attackers will hide—either through skill or dumb luck.

To see how combining different data silos can help find these blind spots, consider any two endpoint technologies—for example, a vulnerability scanner and an agent-based asset tracking system. Each one produces inventories, but in real-world deployments, neither is complete. If you compare their coverage, you will inevitably find gaps or differences.

It can be especially effective to compare data from systems with different objectives—for example, a network-centric feed and an endpoint one. These data silos are normally built by different teams, with different knowledge of the organization and different techniques. When you combine the two, you are likely to find assets known to the endpoint system that come from areas that aren't in your network feed. You may also find the reverse—areas of network that appear to have no endpoints. Comparing data feeds to each other gives you a practical way to address "known unknowns". You can then set up a recurring process to find and fix the coverage gaps in each system based on evidence found in the other, allowing you to bootstrap your way to a far more complete view of your infrastructure, and hence eliminating the dark spaces where bad actors can hide.

Mapping Your Cyber Terrain

To gain a complete picture of your cyber terrain, you need to combine endpoint data with network data. While any comparison of two data feeds can identify gaps, only the combination of network mapping with endpoint data provides end-to-end insight about the state of your defenses. You'll find any gaps in knowledge. Prioritizing assets and identifying issues is also easier when you understand where endpoints are. Something

is probably wrong if a high-value asset shows up in the same part of the network as a group of low priority laptops, or if a user device shows up in a data center.

Building Up Your War Room

So far, we have described the core process that is the foundation of a war room—reviewing business priorities, finding endpoints, categorizing their role, and adding them to a network map. This is also the basis of real-world military mapping—understand the mission, identify assets, then show them on a map. These are steps 1 through 4 of the 10-step recipe for resilience.

Steps 5 and higher take you to the next level of resilience maturity. Once your essential war room platform is in place, you can fold in data from more data silos and technologies to strengthen it and benefit in return. You evaluate each new technology or data silo to answer these questions:

- What does the new data source cover?
- What processing or cleanup does it need?
- What does it add to the map that other feeds did not provide?
- What gaps are there in the new data feed—areas of the map it does not cover?
- How will you respond to any alert conditions from this data source?

Using the War Room to Increase Resilience

The first five steps in building resilience focus on integrating data. The remaining levels add information about particular threats and specific defensive technologies. These advanced disciplines benefit from having a solid inventory with priority assets and locations identified.

For example, consider defense in depth. The concept isn't new, but most organizations struggle to implement more than one or two controls, usually focused controls used on or very near important assets. This is the equivalent of locking a few file cabinets around a building, but not bothering with badge readers to control access into the building. A solid network map with priority assets identified makes it far easier to understand gaps in your defense in depth strategy. Mapping zones allows you to automate the process of tracking zone-to-zone relationships, which benefits compliance as well as network security.

Each new discipline you add to your integrated big picture is enhanced by the war room model, and can add more useful content back into it. The different disciplines can also reinforce each other, as long as they have a common view of your environment (as in the war room), rather than operating in their own data silos with an incomplete understanding of the cyber terrain.

Conclusion

As we've come to understand that perfect protection isn't possible, today's security priority is resilience. Becoming more resilient depends on three key disciplines:

- Being hard to hit
- Detecting rapidly
- Recovering quickly

These goals are best addressed by situational awareness—the result of mapping and understanding your complex, changing infrastructure. The war room model is a time-tested way to visualize your objectives and identify the necessary steps to increase your organizational resilience.

Once this platform is in place, you're ready for the next level—wargaming, or simulating attacks so that you can improve your defenses ahead of the next attack and be prepared for breaches when they inevitably happen.

REDSEAL

940 Stewart Drive, Sunnyvale, CA 94085

+1 408 641 2200 | 888 845 8169 | redseal.net