The Ocden Report on
Cybersecurity Management Anti Patterns

Neha Gupta and Sachin Goyal
OCden Cybersecurity, Oct 2025

The Cybersecurity Management Crisis

Many organizations struggle with the complexities of managing cybersecurity. Despite growing awareness, they find it challenging to keep up with the fast changing threat landscape and fail to build a strong security culture across the organization.

While many factors contribute to the crisis, three recurring issues stand out across industries. These issues are not just technical, they stem from how organizations think, prioritize and operate.

Disconnect Across Teams

Many organizations face a persistent disconnect between cybersecurity teams and business or technical units. Security teams raise frequent alerts, sometimes without a deep understanding of which systems are truly critical. Business and tech teams, on the other hand, often perceive these alerts as exaggerated or misaligned with operational realities. Without a tool to assess risk, or measure impact, differing perceptions of cybersecurity risks persist across teams. As a result, cybersecurity efforts remain fragmented, misinterpreted and deprioritized.

The Compliance Trap

In many organizations, cybersecurity only becomes a priority when customers, partners or regulators demand certifications or proof of compliance. When this happens, organizations often rush to pass audits and get certified. Policies and controls are created to satisfy audit requirements, not to protect systems. As a result, the culture around cybersecurity becomes shallow and transactional. Employees begin to see security tasks as one-time obligations - something to finish quickly without deeper thought. Leadership, on the other hand, reassured by a compliant status,

assumes all is well and fails to probe deeper. Thus, despite meeting compliance standards, the organization remains vulnerable.

Lack of Executive Ownership

While leaders of most organizations recognize the importance of cybersecurity, many struggle to embed it into core business planning. As a result, cybersecurity efforts often get sidelined by more visible, immediate priorities like revenue growth, product delivery, etc.

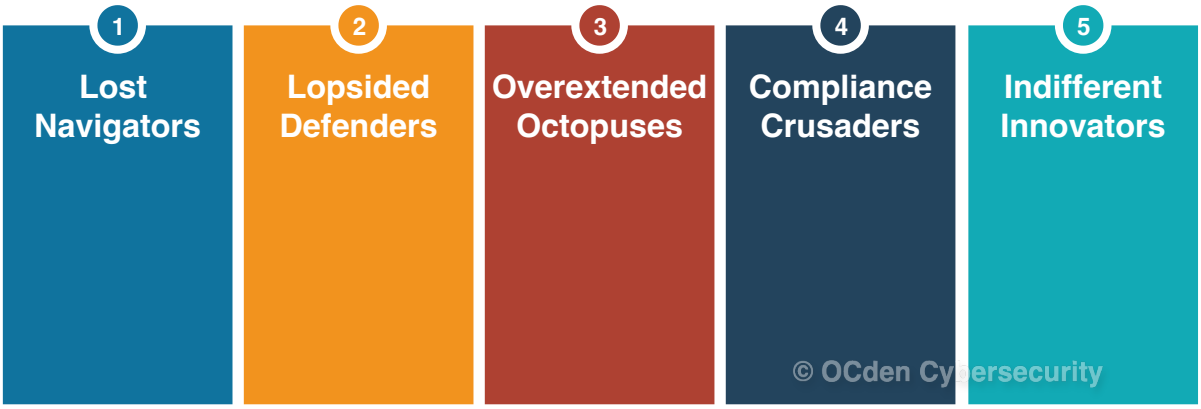
The First Step: Organizational Self-Awareness

To move beyond this impasse, organizations must understand their current posture in terms of how they operate and where they struggle. Yet this kind of introspection is nearly impossible without a shared lens - one that allows all levels and teams to view the organization through a common framework.

To address this need, we've identified recurring anti-patterns i.e. consistent struggles observed across organizations in our cybersecurity engagements. The purpose of identifying such patterns is to provide a shared lens through which stakeholders can visualize and discuss the dynamics within their organization. This common language helps bridge perspectives: while top management may attribute one pattern to their organization, the security team might see another. That divergence is not only natural but valuable. These patterns offer a framework for more aligned conversations to reflect and act.

Organizational Anti-Patterns in Cybersecurity Management

We can broadly categorize the struggling companies into the following patterns:



> ⚠ **Note**
>
> Before we examine these patterns, it's important to note that they are neither mutually exclusive nor exhaustive. Organizations vary widely in terms of industry, maturity, regulatory pressures and internal dynamics. As a result, additional patterns may emerge, and in many cases, multiple patterns may coexist within the same organization.

1 Lost Navigators

These organizations don't have a clear cybersecurity strategy. So when a breach hits the news or a customer demands action, they resort to reactive measures like jumping between tools and processes in search of quick solutions or chasing the latest cybersecurity trend. And when they finally try to adopt a framework like ISO 27001 or NIST CSF , they feel paralyzed. The scope feels massive, and without the basics in place, it's hard to know where to start.

Lost Navigators struggle because they haven't laid the necessary groundwork like identifying crown jewels. They try to implement all controls from the frameworks which leads to a patchwork of quick fixes that are temporary and fragile. They can do better by adopting the risk based approach, where cybersecurity efforts are prioritized based on the criticality of assets and the severity of threats they face. Basically protecting what matters most rather than applying blanket controls.

2 Lopsided Defenders

These organizations usually have leadership support and generous budgets, still they miss the mark on cybersecurity. They lack a deep understanding of their own infrastructure and often fall for sales pitches that oversell costly, high-tech cybersecurity solutions. It leads to securing only a few systems while many other critical entry points remain vulnerable. The danger isn't what's visible - it's what's ignored.

Lopsided Defenders keep layering the latest "fix-everything" technology over last year's "fix-everything" technology. No amount of AI or automation is going to make a real difference until they nail the basics like understanding their own environment and unique risk landscape before investing in the next big technology.

3 Overextended Octopuses

These organizations have their tentacles reaching in every direction to cover all bases. This is typically seen in large and established companies. They mistakenly believe that every cybersecurity risk should be resolved immediately, which leads to unnecessary stress and conflicts with other essential business functions.

Overextended Octopuses eventually find themselves overwhelmed by too many security measures, leading to employee frustration, reduced productivity, and ballooning budgets. They can do better by adopting the risk based approach, where they identify and score risks. This ensures that the most pressing risks are handled first. Less urgent risks can be deferred, and exceptions may be applied when they interfere with critical business operations.

4 Compliance-Driven Crusaders

These organizations focus solely on meeting standards and obtaining certifications. They want to check the boxes with minimal effort and least impact on existing systems. They even tend to choose auditors who lean heavily on paper work and focus less on the actual implementation of controls. Some of these organizations even go as far as to ‘buy’ certificates for a ‘hassle-free experience’.

This narrow focus on getting certified creates a false sense of security within organizations. It breeds complacency, causing teams to overlook real security needs thereby leaving critical systems exposed and vulnerable to attacks. They can do better by investing time and energy in strengthening cybersecurity fundamentals like identifying crown jewels, mapping risks and aligning priorities. Once the foundation is solid, certifications will follow naturally.

5 Indifferent Innovators

These organizations wonder why they should get involved in the complexities of cybersecurity. To them, cybersecurity seems like an unnecessary burden, something that can be ignored until they are bigger and more established. These companies think they’re too small to attract hackers and hence avoid efforts on security. It is like people not bothering to lock their doors because they believe thieves will go after the bigger and wealthier homes out there. But unlike physical theft, cybercriminals operate at scale - 99% of cyber attacks are automated, seeking out any weakness, regardless of the size of the business.

Indifferent Innovators can do better by starting small and keep on building maturity over time. This steady approach ensures that when the need arises (like customer or regulator demand), the groundwork is already in place, ready to support swift, informed action rather than reactive scrambling.

Cybersecurity Management: An Iterative Approach

In many fields like software and design, an iterative approach is the norm. Work evolves over time, refined through cycles of learning and adjustment. Yet in cybersecurity, this mindset is surprisingly rare. People often treat it as a binary switch: either you're secure or you're not, certified or not certified. In reality, cybersecurity maturity is best achieved through continuous improvement where organizations build, assess and improve year after year. A rough roadmap for this iterative approach includes three essential pillars:

- **Establishing the Foundation**

  Organisations should have an understanding of their *critical assets and associated risks* - especially what are their crown jewels and what's the current state of security controls in place. When this happens, controls and safeguards are implemented in response to actual risks, not just to satisfy frameworks or compliance checklists.

- **Directing the Effort**

  Organizations should adopt *a risk-based approach to cybersecurity prioritization* and align it with overall business planning. All cyber risks are not equal and they don’t affect every organization in the same way. Business context matters and cybersecurity strategies must reflect that. Once cyber risks are scored and prioritized in the context of overall business plan, it becomes easier to align the efforts across the organization.

- **Equipping the Team**

  Organisations should cultivate *a security-conscious culture* where every individual understands their role in protecting the organization. This means embedding cybersecurity awareness into daily routines and fostering a sense of shared accountability. This is achieved through role-specific trainings, consistent reinforcement of security practices and strong leadership support.

Concluding Remarks

OCden Cybersecurity has interacted with multiple organizations, both small and large, to understand and help improve cybersecurity management. We have seen the most success when engagements start with the top - for example, with a cybersecurity leadership training for top executives. This sets the tone for enterprise-wide commitment. These organizations adopt a structured approach, focused on identifying and executing a prioritized list of action items year after year. They view cybersecurity maturity not as a fixed destination, but as a continuous journey of improvement.

We, at OCden Cybersecurity support this journey with a comprehesive set of tools for risk management, policy & control management, culture building, and help tie it seamlessly to achieve required compliances. Regular oversight through OCden platform ensures progress is tracked and priorities are adjusted as needed. You can find more details at ocden.com