Capgemini

CYBERSECURITY RESILIENCE

Rebuilding IT operations to emerge stronger post-crisis

The outbreak of COVID-19 has upended nearly every aspect of life, from the personal aspects of how people live and work to changes in the professional world. The changes in the business world encompass changes to how companies interact with their customers, how customers choose and purchase products and services, and how supply chains deliver them. Numerous studies and surveys suggest that we will see a fundamental change in the way people do business over the next five years, with many asserting that the crisis will have a permanent lasting impact on both their own operations and customers needs. Common to most of the presented visions for future business dynamics is an increased focus on digitalization and IT investment.

This in turn poses an unparalleled cybersecurity challenge, the rapid adoption of new IT-based technologies has historically led to rapid accumulation of technical debt and designs which have proven to embed server cybersecurity risks. However, the crisis also offers the chance for a new beginning – a chance for businesses to rebuild their IT operations and emerge post-crisis with a strong and resilient cybersecurity foundation.

Here's Capgemini's take on three ways to position your organization's cybersecurity efforts to emerge stronger in the post-crisis world:

1. Ensure security investments result in relevant capabilities

Today, cybersecurity is no longer regarded as a function of the IT department, it is everyone's responsibility. Modern attacks now take place on multiple levels. With so many potential points of attack, the key to improving security is to create a culture of healthy suspicion. Everyone has a role to play and ensuring that the security function has appropriate human capital and partnerships in place is vital.

Too often, companies invest in cybersecurity tools, but neglect to align the employee's behavior and the organizational structure within which these tools will be employed. Instead invest in training and build a strong security culture, only choosing tools which give you awareness and insight that is relevant for securing you business operations. Communicate your goals clearly and ensure that the information you expect to gain from improved tooling actually enables effective action within the structure and abilities of the organization you are trying to protect.

For example, investing in expansive Security Information and Event Management Solutions (SIEM) systems and security analytics that provide real-time insight into threats may seem like a major step forward. However, without aligning this investment with internal security teams and training them to respond effectively, organizations may end up watching helplessly as a crisis unfolds while being unable to act effectively. Instead adopt a risk-responsive approach that ensures that the kind of response you can mount is aligned with preserving key business capabilities. Invest in analytics only at the pace your security teams can evolve to act on the increased sources of information. Having a lot of data about security, which you are unable to act on is not an improvement of your security posture.

2. Evolve faster than the attacker

In the words of renowned security guru Bruce Schneier: "Attacks always get better". In cybersecurity, we are up against intelligent attackers. Hackers are constantly adapting their techniques and finding new ways to penetrate our systems, evolving to take advantage of new trends and online behavior. This is fundamental to being successful as a cyber-attacker and frequently cybercriminals and other adversaries are at the forefront of innovation. Indeed for many corporate IT-managers their first encounter with new ideas like cryptocurrency are when they are confronted by the demands of a ransomware attack, a category of attack which has seen a significant rise as attackers use COVID-19 as the basis for deceiving employees and customers into unsafe behaviors.

The concept of trying to evolve faster than attacker has been extensively studied in military circles where the notion an OODA loop (see figure 1) has emerged as a grand unifying concept in trying to prepare for the next conflict as opposed to last. In this cycle, organizations must seek Observe, Orient, Decide and Act against cyber threats, such that all decisions are based on observations of the evolving situation tempered with implicit filtering of the problem being addressed. The observations are the raw information on which decisions and actions are based. The observed information must be processed to orient it for decision making. The second O, orientation – as a repository of an organization's heritage, cultural traditions, and previous experiences – is the most important part of the OODA loop since it shapes the way we observe, the way we decide, and the way we act.

In order to win, we should operate at a faster tempo or rhythm than our adversaries. Ideally, we seek to get inside the adversary's OODA loop. Such activities will make an organization appear unpredictable to an attacker thereby generating confusion and disorder among adversaries since they will be unable to generate mental models that agree with the faster transient rhythms or patterns they are competing against. By taking this organizational approach one can build resilience, rather than making plans for every eventuality, developing systems and procedures that are flexible. Focus on capability and operational tempo, not on specific defenses.

Further, make use of cyber intelligence to gather information that informs: what might some malicious actor do to disrupt business operations and how can we defend against it? When investing in new cybersecurity capabilities take a dynamic, learning approach that keeps up with the pace of innovation.

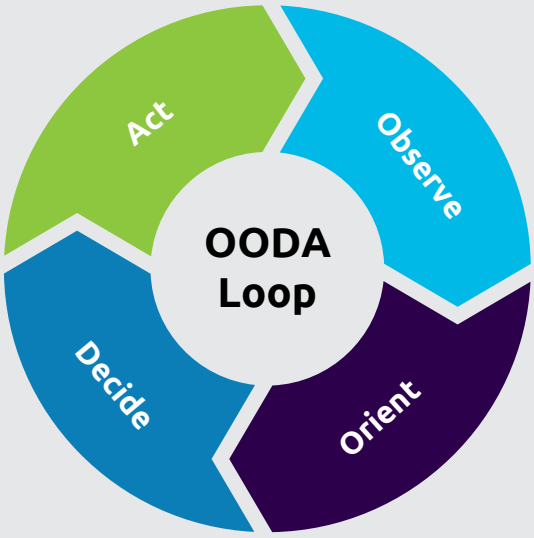


Fig. 1

Observe
What is the current situation? What is the reason you want to change? How bad do you want to change?

Orient
Where are you currently at relative to where you want to go? How far is it to your destination?

Decide
What is the exact path you are going to take? How are you going to handle challenges and set backs?

Act
What's the approach and method you will take to implement the decisions? What is your action plan?

3. Think long-term and exploit emerging security technologies

While cyber security threats will always exist, the long-term focus in cybersecurity should be on improving the fundamental security properties of the systems we seek to protect. Writing code that is secure and without vulnerabilities, is a critical challenge to cybersecurity, but is at least as difficult as writing code without bugs. While there are many other potential sources of security exposures in software, developing code without known classes of vulnerabilities has become an achievable goal. It relies on human developers using tools, techniques, and processes to produce software that by design cannot contain certain particular known types of defects.

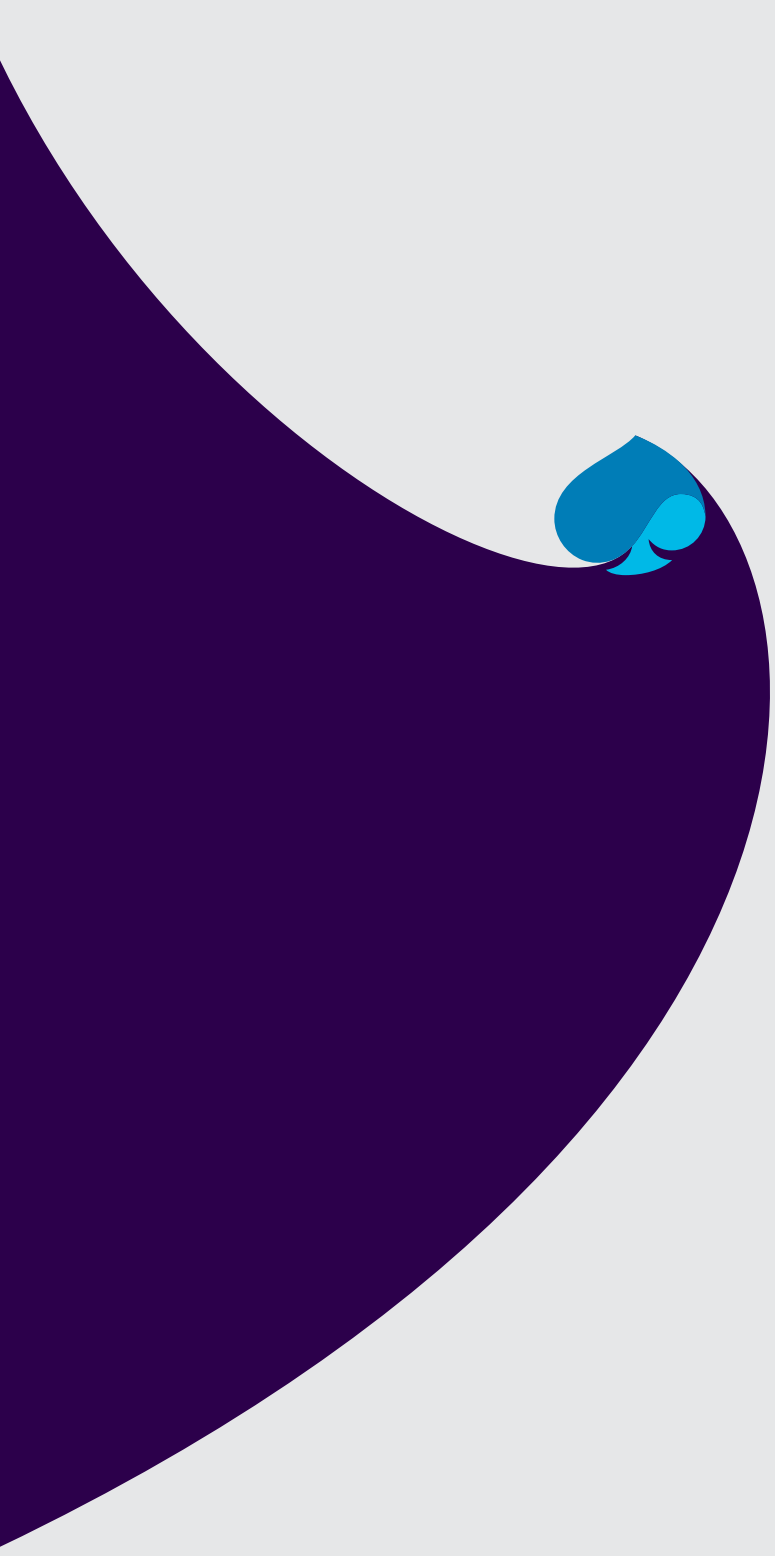
Research into programming languages and tools, has yielded technologies that are proven to resist categories of vulnerabilities, largely by not allowing for them. Memory safe languages that manage memory allocation and deallocation, instead of requiring the programmer to do so, make it impossible for developers to create buffer overflow vulnerabilities and some other types of exposures, from missing array bounds checks, null pointer use, and data leakage via memory reuse. Thread-safe languages can address exposures where race conditions can be used to subvert security-related checks in the program.

Within the software development community, groups and organizations with a mission to develop software securely have incorporated tools and techniques into their software development life cycles to include a secure development life cycle. A modern secure software development lifecycle that incorporates root cause analysis, security education, threat modeling, specific secure coding requirements, and security testing that includes penetration and fuzz testing, does produce systems which are far less vulnerable that the typical systems encounters today. However, practices tend to be adopted based on business need, perceived security impact, and fit with established or evolving development practices. An effective security leader must not only understand both these technical trends but also the organizational dynamics that must be changed to enable such technologies to be adopted.

Conclusion

While the long-term implications of COVID-19 remain unknown, companies should focus on building a flexible and resilient cybersecurity foundation that will allow them to emerge stronger, smarter and ready to exploit new technologies post-crisis. In particular, investments that enables security teams to be more agile and which allow for security by design will provide sustained long-term returns.

Find out how Capgemini can help you, visit us at: https://www.capgemini.com/service/cybersecurity-services/



About Capgemini

Capgemini is a global leader in consulting, digital transformation, technology and engineering services. The Group is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year+ heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. Today, it is a multicultural company of 270,000 team members in almost 50 countries. With Altran, the Group reported 2019 combined revenues of €17billion.

Learn more about us at

www.capgemini.com

People matter, results count.