ADAPTIVE DEFENSE

A CAPABILITY MATURITY MODEL FRAMEWORK

Publication Partner

The Kosciuszko Institute

EUROPEAN CYBERSECURITY SPECIAL

This publication will be openly distributed to interested parties and stakeholders, and available in the January edition of the European Cybersecurity Journal, in order to foster the debate on cybersecurity management and policy making.

FOREWORD

STEVEN WILSON
Steven Wilson is the Head of the Europol Cybercrime Centre (EC3). He was the Scottish representative on UK cyber governmental and policing groups and led on industry and academic partnership groups on cyber resilience in Scotland.

DR. JOANNA ŚWIĄTKOWSKA
Dr. Joanna Świątkowska is the Programme Director of the European Cybersecurity Forum, the Chief Editor of the European Cybersecurity Journal and Senior Research Fellow of the Kosciuszko Institute. She is a member of the Advisory Group for Cybersecurity of the Republic of Poland working within the Polish Presidential National Bureau of Security (NBS).
joanna.swiatkowska@ik.org.pl

AUTHORS

ADAM PALMER
Adam Palmer, CISSP, JD, MBA, is a global cybersecurity policy and strategy leader. Adam is a former US Navy Officer, Prosecutor, and Manager of the U.N. Global Programme Against Cybercrime.
adamppalmer@gmail.com

DR. PHILIPP AMANN
Dr. Philipp Amann, MSc, is the Senior Strategic Analyst, Head, Strategy Development Team at the EUROPOL, European Cybercrime Centre (EC3).
philipp.amann@europol.europa.eu

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute. Authors may have consulting or other business relationships with the companies they discuss.

Executive Editor: Karine Szotowski **DTP:** Marcin Oroń

FOREWORD

STEVEN WILSON
Head of the European Cybercrime Centre

From a law enforcement perspective, the current cybercrime landscape is characterized by increasingly aggressive and confrontational behaviour; attacks are becoming cross-platform compatible, more targeted, growing in scope, volume, number of victims and economic damage.

Cybercrime is now also being "industrialised" and is characterized by a division of labour with specialisation of specific services. This is driving a digital 'Cybercrime as-a-service' (CaaS) underground economy. This CaaS model represents a continuously evolving and modular industry that facilitates cybercrime and stimulates the innovation of tools and methods. By enabling a broad base of often unskilled, entry-level criminals and other actors to launch cyber attacks, the CaaS model gives disproportionate capabilities to attackers and creates an asymmetric risk for organizations in terms of risks, costs and criminal profits.

The growth of cybercrime and the increasing damage caused by attacks calls for innovative law enforcement approaches to prevention, protection and investigation. Such approaches not only need to be intelligence-led, agile and adaptive, but also require efficient public-private partnerships to respond to the dynamic, evolving and borderless nature of cybercrime in an equally diverse, coordinated and flexible manner.

An important aspect of public-private partnerships is the sharing of intelligence in a structured and standardised way among all relevant stakeholders with a view to building a comprehensive intelligence picture of cyber threats. This requires a common understanding of the type and category of intelligence that needs to be shared and its purpose. Equally important, it requires mutual trust as well as confidence by industry in law enforcement's ability to investigate both effectively and discretely.

For industry, besides establishing a base line cybersecurity and cyber resilience, a key strategic objective should be the adoption of a holistic and intelligence-led approach to protect and defend against cyber threats. This paper offers a systematic approach to achieving this by leveraging existing maturity model approaches to realise the ideal security posture of an Adaptive Defence. It describes a sustainable and resilient model that includes a circle of detection, prevention, analysis, and effective incident response to threats, underpinned by a continuous learning and improvement cycle.

Public-private partnerships and the systematic sharing of intelligence are some of the key aspects of an Adaptive Defence. The model specifically highlights the important role law enforcement plays in this context. It also supports novel and innovative, intelligence-led law enforcement responses to the growing threat of cybercrime and cyber threats in general.

PREFACE

DR JOANNA ŚWIĄTKOWSKA
Chief Editor of the European Cybersecurity Journal
CYBERSEC Programme Director
Senior Research Fellow of the Kosciuszko Institute, Poland

The very nature of the digital world stands in clear contrast to such words as stability, rigidity, or hierarchy. The Internet is dynamic, decentralised, and flexible, where different parts of the system interact with each other and are interdependent. By using a similar contrasting analogy, we can also capture the characteristics of actions aimed at ensuring safe cyberspace. In order to achieve a high level of cybersecurity we should act in a comprehensive and proactive manner as passive and one-dimensional thinking is doomed to failure.

Presented in this article, the approach referred to as "Adaptive Defense" is a good example of such effective and modern action. We need to be aware that only by taking into account the most important elements of the entire lifecycle of cybersecurity assurance – namely, detection, prevention, analysis, and effective incident response to threats, we stand a real chance to effectively counter the increasingly sophisticated and serious threats. The need to put emphasis on building a broadly defined strong and multidimensional cooperation between the various stakeholders is no less important.

An extremely important feature of the "Adaptive Defense" is that it can be deployed in any kind of organisation, both at the level of a single enterprise as well as in entire countries.

From the point of view of public bodies, adopting a model approach will be very useful, not only at the stage of determining the strategic framework for cybersecurity, but also enhancing the already adapted strategies. In fact, now is a perfect time to start employing benchmark solutions because many countries, including European states, are currently in the phase of either producing or updating their key documentation. Built upon the risk management process, an appropriate identification of key processes, relations, roles, and responsibilities significantly increases the chances of success of the project called cybersecurity capacity-building.

Similarly, at the level of individual enterprises and organisations, the deployment of solutions that increase active defence capabilities is the only legitimate way to move forward in order to win the race against increasingly complex and persistent threats. The actors that are particularly vulnerable to these kinds of threats are those composing critical infrastructure, i.e. businesses whose smooth operation determines the security of entire nations. Therefore, it is of fundamental importance to promote solutions that build cybersecurity across all levels of the organisation also in this area.

I. OVERVIEW OF THE THREAT LANDSCAPE

While cyberattacks are becoming more advanced, the goal often remains the same – to steal information or money as quickly as possible. Attackers include state-sponsored threat actors or organized crime. While motivations may differ, the tools used are similar. Tactics, Techniques, and Procedures (TTP) may include social engineering, phishing, extortion, or malware attacks such as ransomware.

One recent report on a financial crime group provides a clear example of both advanced attacks and spearphishing. This crime group systematically targeted financial information in the biomedical and pharmaceutical sectors. The group used targeted and sophisticated emails to lure victims, who included CEOs, CFOs, research scientists, and lawyers, into providing their email credentials. The attackers then inserted themselves into the email trails, gaining access to privileged and market-sensitive information that would significantly impact the market value of the target companies. The attacks were successful without the use of any malware, relying on users to unwittingly use their email credentials on systems under the attacker's control. A lack of two-factor authentication on target victim systems made these attacks surprisingly simple yet highly effective.

Some attacks are now conducted without any malware. One example is when attackers leverage stolen credentials to access virtual private networks (VPN) infrastructure and connect to a network appearing to be a legitimate user. This can occur where attackers have successfully infiltrated the network in the past, and then compromised the domain credentials – in some cases, even compromising the two-factor authentication used for secure VPN connections. This allows attackers to return into the network using the corporate VPN, disguised as legitimate users thereby making detection difficult.

The recently discovered "CoreBot" malware is an example of the sophistication of social engineering attacks. CoreBot, a relatively new form of banking malware, uses a modular design that allows threat actors to customize the malware for different victim networks, as well as to install features, as needed, during an intrusion. CoreBot can perform browser injection, form-grabbing, and credential theft. It also includes a social engineering component to gather personal details from victims, information that is typically used as a secondary form of verification by financial institutions. This additional functionality may lead to higher success rates for financial fraud, identity theft, and even future social engineering attacks.

Attacks have also expanded to mobile devices. Researchers recently identified a series of Android trojan apps that are aimed at defrauding financial management institutions and service providers across the globe (North America, Europe, and Asia Pacific). Nicknamed "SlemBunk", these apps masquerade as common, popular applications and stay hidden after the initial running. They have the ability to phish for and harvest authentication credentials when banking and other similar apps are launched.

The continued sale and distribution of exploit kits and many spam campaigns demonstrates that attackers are still seeking easy compromises similar to "smash and grab" physical crimes in which the attackers do not intend to expand access beyond the infected system. While some exploit kit activities link to more advanced threat actors, the majority are associated with mass exploitation campaigns for monetary or personal information gain. Estimates of the cost of these threat activities are difficult to obtain and vary, but billions of U.S. dollars are likely lost globally. In some more egregious cases, there are lasting effects, where affected organizations realize the financial and reputational impact of compromises over the course of years. Though many of these attacks are opportunistic, some cybercrime actors may attempt to sell access to infected networks. Once access is sold, the activity may shift from opportunistic to a targeted attack.

Many cybercrime activities are facilitated by a professional underground "cybercrime as-a-service" industry that provides easy access to criminal products and services, and enables a broad base of often unskilled, entry-level criminals and other actors to launch cyberattacks. This gives disproportionate capabilities to attackers and creates an asymmetric risk for organizations in terms of risks, costs and criminal profits.

From a law enforcement perspective, the cybercrime landscape is characterized by increasingly aggressive and confrontational behavior. Specifically, law enforcement observes an increase in:

- ransomware and cryptoware
- use of remote access tools (RATs)
- card-not-present (CNP) fraud, which is likely to increase further since traditional cash-out destinations (like the U.S.A) for card-present (CP) fraud are starting to implement the EMV standard
- banking malware: targeting customers, but also banking infrastructure directly
- ATM malware: physical and logical attacks against ATM machines and ATM networks
- mobile malware
- social engineering

> " From a law enforcement perspective, the cybercrime landscape is characterized by increasingly aggressive and confrontational behavior.

Law enforcement has also observed the increasing criminal abuse of encryption and anonymity services and tools to mask identity and physical location, hide data, protect communication and obfuscate financial transactions. These developments call for an equally advanced, adaptive and holistic strategic approach as recommended by the Adaptive Defense model.

II. ADAPTIVE DEFENSE AND THE CAPABILITY MATURITY MODEL

A Capability Maturity Model (CMM) provides an organizational framework and methodology to build capacity and measure advancement in critical areas of cybersecurity. Maturity models are useful in guiding the development of processes and allocation of resources leading to an optimal state of readiness for a strategic objective. They can help assess current capability levels and identify areas of improvement using a risk-based assessment. Maturity models are also useful for evaluating compliance in the relevant legal and regulatory environment and for facilitating forward-looking analysis or "horizon scanning" for new emerging concerns and requirements.

Leveraging existing maturity model approaches[1] and related work[2], this paper offers additional, more granular, suggestions for achieving the ideal security posture of an "Adaptive Defense". The term "Adaptive Defense" summarizes a strategy that includes a holistic circle of detection, prevention, analysis, and effective incident response to threats, underpinned by a continuous learning and improvement cycle (capacity building). An Adaptive Defense describes a strong, sustainable and resilient model that also provides for a flexible approach to cybersecurity.

Benefits of using a CMM to develop an Adaptive Defense include:

- Establishing a holistic implementation framework with broad functionality
- Obtaining a snapshot of current readiness against various levels of maturity
- Within a broader strategy, providing for a flexible

[1] | Cyber Security Capability Maturity Model v1.2, Global Cyber Security Capacity Centre, University of Oxford, December 2014, available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20Version%201_2_0.pdf.

[2] | Bodeau, D. J. and Graubart R., Cyber Resiliency Engineering Framework, MITRE Technical Report, September 2011, available at: https://www.mitre.org/sites/default/files/pdf/11_4436.pdf.

approach that can be modified as technology or threats evolve
- Promoting a dynamic assessment and continuous improvement cycle

The most important concept of the CMM and Adaptive Defense is that each organization will have a specific goal level on the readiness spectrum. The goal will adapt according to changes in an organization's internal and external risk-based assessment. Part of the benefit of the CMM is the actual process to identify critical capability areas (domains) that correlate with a desired security readiness outcome. An organization should identify maturity levels within each domain. These are established by assessing the status quo and measuring progress along a continuum of risk-based preparedness from low readiness levels to full Adaptive Defense capability. The organization using a CMM should benchmark existing cybersecurity preparedness, evaluate core competencies, and create a framework that dynamically manages and measures improvement.

> “ The term “Adaptive Defense” summarizes a strategy that includes a holistic circle of detection, prevention, analysis, and effective incident response to threats, underpinned by a continuous learning and improvement cycle.

Maturity level metrics provide a foundation for creating specific recommendations to increase capacity in areas of clearly identified need. Applied at the nation-state level, a CMM allows an aggregated view that can be gradually refined and expanded to all relevant national agencies, ministries, and stakeholders. Goals are likely to differ based on the characteristics of an organization such as size, structure, risk posture, and so on. There is not a "one size fits all" approach. The correct goal or appropriate maturity level for any domain must be based on the specific needs of each organization, consideration of the overall strategic objectives, and any relevant legislative and regulatory framework.

The heart of an adaptive defense is a dynamic and iterative process. It encourages holistic solutions and flexibility to achieve the appropriate levels of cyber resilience and readiness levels. The CMM approach supports organizations in building core capabilities by utilizing a defined methodology to steadily improve readiness levels. This is a bespoke approach. It focuses on specific risk areas and helps an organization ensure alignment across different domains. Narrowly tailored solutions can be applied to achieve specific measurable outcomes. By providing an accurate view of current readiness and a pathway toward improvement, the CMM process provides an operational framework for achieving an Adaptive Defense.

The core Adaptive Defense domains include Resilience, Detection, Coordination, Capacity, Cooperation. Each of these domains will be described in the following section and covered in more detail in section IV, which proposes a CMM-based approach to achieving an Adaptive Defense.

III. THE ESSENTIAL ELEMENTS OF AN "ADAPTIVE DEFENSE"

Resilience

Although cyberattacks are inevitable, an organization should have a defense that allows operations to continue with minimal disruption, and that provides adequate protection for critical assets. A data breach should not become a major "security incident". An organization must also learn from such events with a view to improving readiness levels. This is a form of resilience. Resilience is the ability of an organization to adapt to change and new risk environments, and to gain intelligence from past attacks. Resilience is not a single technical domain but a multi-faceted and multi-disciplinary domain. It includes the ability of an organization to not only prepare for and detect security threats, but to respond effectively in a timely manner, minimize damage, withstand disruptions, and to learn and adapt. If an organization takes weeks or months to mitigate a breach once it is detected, it has poor resilience.

Prevention is part of an Adaptive Defense. The resilience domain also includes prevention, but detection and effective incident response are the keys to resilience. The resilience domain has a broader scope than basic "cyber hygiene" security. These are related, but separate, concepts. The U.S. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience defines "security" as reducing the risk by implementing defensive measures. "Resilience" is defined in the same directive as the ability to prepare for and adapt to (detect) changing conditions as well as the ability to withstand and recover rapidly from disruptions. Detection and incident response are the critical differentiators of resilience from mere defensive security. Frameworks that include resilience-based standards and recommendations include the ISO standards, the NIST U.S. security management framework and the Cyber Resiliency Engineering Framework[3].

Detection

Security includes not only identifying known threats, but the ability to detect and prevent unknown threats. An organization cannot prevent threats if it does not identify or detect a threat. The detection domain includes the response to threats once they are detected. Detection is the ability to make decisions based on a flexible programmatic approach that is based on actionable real-time information. This reduces mass amounts of information to focus areas based on direct understanding of threat actor methodologies and likely attack vectors.

Moreover, detection comprises the learning capabilities of an organization in terms of identifying and responding to threats. Managing intelligence and applying the knowledge gained from intelligence sources are critical in establishing adequate security and an Adaptive Defense. As such, detection is closely linked to resilience.

Coordination

Cybersecurity requires a multi-stakeholder and multi-faceted approach that is a harmonized response across multiple capability areas. The coordination domain includes organization of internal personnel, equipment, facilities, and plans necessary for collaboration and synchronization in planning for cybersecurity activities. This domain focuses on overall harmonization across an organization's security planning and response strategy both internally and externally. It also addresses questions of standardization, timeliness, and level of detail, and aims at enabling stakeholders at all levels.

Coordination is supported by clearly defined communication protocols; common taxonomies and standards for the description, exchange, and (automated) processing of information and intelligence. Coordination should include the creation of clearly defined points of contact for exchange of threat intelligence and

[3] | Op. cited Bodeau and Graubart.

management of risk mitigation activities – an example would be the merger of the Security Operations Center (SOC) and the Computer Incident Response Team (CIRT). Coordination is essential for effectively pooling the response capabilities of various stakeholders and avoiding conflict. A sound security plan should include mutually reinforcing activities that are synchronized across an organization. These activities should establish a front line of defense against immediate threats by enhancing shared situational awareness of network vulnerabilities, threats, and risks. By coordinating a security strategy across an organization, the organization increases its cyber resilience, strengthens its security environment, and reduces the risk of a threat causing significant harm.

Coordination is also a measure of organizational efficiency. Coordination can save costs by identifying operational areas that may be scalable and by avoiding unnecessary overlap and redundancies. During an evaluation of organizational needs, it may be possible to identify areas of commonality where the organization can implement shared controls or processes. This can avoid duplication and improve assurance that systems will be compatible. All of these activities improve the resilience and responsiveness or readiness of an organization.

Capacity

The capacity domain encompasses the ability of an organization to implement and execute its security strategy effectively. It is a measure of an organization's ability to promote the scale, quality, and implementation of cybersecurity initiatives across the organization. Using a risk-based approach, an organization may find that not every organizational entity needs to be at the same level of protection. Some entities may be categorized as "cyber key terrain" (CKT) assets. Capacity goals are adjusted within the maturity model based on an outcome of the risk-based assessment and identification of CKT.

A critical element of the capacity domain is the participation of senior decision makers across an organization to gain a clear understanding of CKT, security needs, and support for solutions. Capacity building should encompass not only vertical staff training but also horizontal efforts across an organization, focusing on the relevant aspects at each organizational level and in each functional area that are needed to support the security programme.

"Escalation" is a term now used in cybersecurity to describe the concept of an attacker entering a weak area of an organization's network and moving laterally into more secured areas. Because attackers have had devastating success using escalation to access and control networks, it has now become cliché to define an organization as only as strong as its weakest part. Coordination is critical to ensure that an acceptable cybersecurity baseline is established and that cybersecurity is harmonized at a necessary standard across an organization.

Cooperation

Public-private partnership (PPP), including cooperation with industry partners, the financial sector, academia, and law enforcement, plays an important role in increasing cybersecurity and resilience through raising awareness of threats, improving the overall intelligence picture, leveraging cybersecurity networks, and preparing adequate support for an effective response. Law enforcement, in particular, can be an effective partner that goes beyond detection. Successful cooperation and support for law enforcement operations can help tackle some criminal networks. Cyberattacks will likely continue to grow in volume, scope, impact, and level of sophistication. The borderless nature of the attacks makes PPPs essential to address these unique challenges. A PPP model based on mutual trust, efficiency and effectiveness is needed whereby an organization will feel comfortable sharing information with government, and law enforcement investigates incidents discreetly and effectively. Accordingly, cooperation is a key to a successful Adaptive Defense.

IV. ACHIEVING AN ADAPTIVE DEFENSE

This section examines each core Adaptive Defense domain in detail. It is suggested to apply and evaluate each domain utilizing the CMM multi-stage evaluation process.

Applying The Capability Maturity Model

The initial analysis and planning for applying the CMM should include:

1. Conducting an assessment of each current operational area and its place on the CMM scale
2. Coordinating with internal stakeholders to apply a risk-based approach to establishing and evaluating the appropriate readiness level for each area
3. Identifying the steps necessary to move each area to the required level of security readiness
4. Identifying the ongoing requirements to maintain the appropriate readiness levels
5. Establishing an audit system with reporting requirements to verify maintenance of standards, identify deviations, and implement necessary adjustments on an ongoing basis
6. Implementing appropriate incentives and penalties
7. Providing appropriate protections of privacy and human rights
8. Establishing a long-term plan for building and maintaining capacity

Not every operational area within an organization needs the most advanced security. Identifying "security zones" or CKT is critical to identifying groups or assets that are worth defending or whose loss would be disruptive. Answering the questions "how good do you need to be", and "what type of cyber risk management program do you need" should be part of a collaborative discussion across all the relevant stakeholders in an organization. This should include the identification of all critical assets. The modular step-by-step design of the CMM and not placing all groups in a single readiness track is intentional. There is a range of possible activities for each domain and these will vary across each organization – this is the foundation of a risk-based approach to creating an adaptive defense.

This approach is designed to enable a comprehensive, long-term, adaptive, and holistic approach to preventing and combating cyber threats and establishing a security readiness baseline. The focus is placed on understanding existing capabilities, ensuring that current initiatives are not duplicated, and implementing the necessary measures to assure long-term success.

A. Resilience

Resilience is the foundation of an effective cybersecurity programme – be it at national or organizational level. For the purpose of this paper and in support of the creation of an Adaptive Defense, resilience consists of four core areas:

1. Detection: Detection includes planning to evolve a security program beyond "basic cyber hygiene" to include intelligence from a range of sources and to make programmatic decisions based on actionable relevant information.

Threat intelligence should include awareness of known threat groups, their known attack methods, and anticipated attack vectors. Identifying the source of an attack can help you understand the objectives and motives of the attackers and why they are targeting your organization. From an Adaptive Defense standpoint, this means that security programmes should evolve from passive monitoring to active "hunting" for evidence of threat actors within a network. This approach assumes the presence of an attacker that is using unknown intrusion techniques.

While intelligence can be considered one of the main elements, detection also encompasses other types of sources, producing different types of input, including data and information as well as intelligence, which typically involves human resources and interpretation. However, automation using artificial intelligence, machine learning, and Big Data analytics will play an increasingly important role in these areas and Adaptive Defense in general.

Essential elements of the detection domain are:

- Dynamic defenses to stop targeted, zero-day attacks, leveraging machine learning approaches
- Real-time protection to block data exfiltration attempts
- Integrated inbound and outbound filtering across protocols
- Accurate mechanisms that ensure a low false positive rate
- Global intelligence on advanced threats to protect local networks

To be effective, detection must be "intelligent" enough to identify and stop advanced polymorphic attacks hosted on dynamic, fast-changing domains. To address these advanced threats, real-time, dynamic and accurate analysis of network traffic and processes is critical. A fully mature Adaptive Defense aims to dynamically recognize new attacks in real time, without necessarily requiring prior knowledge of vulnerability, exploit or variant, and then prevent system compromise and data theft. This includes stopping data exfiltration and the ability to dynamically analyze network traffic to capture and detect zero-day malware. Equally important are real-time capabilities to stop the outbound communications of an attack and halt the flow of data to attackers. This needs to include advanced techniques to counter modern forms of steganography and other types of information hiding techniques in network traffic.

2. Prevention: Prevention includes activities to stop known and unknown threats from becoming security incidents. These activities include, among other things, protocols that are essential to a security programme and additional behavior-based heuristic detection capabilities that can prevent an attacker from exploiting an unknown vulnerability. Prevention includes a human dimension that focusses on minimizing threats and risks related to human behavior and exploits (such as social engineering) as well as learning and education.

Some of the main sub-domain controls for prevention and detection are:

- Asset management (including cyber key terrain)
- Upgrade/patch management
- Vulnerability management
- Vulnerability scanning and system testing
- Heuristic detection and analysis, machine learning, and data analytics
- Organizational and individual training and education to minimize the risk of social engineering (this reduces but does not eliminate the risk)

Traditional approaches to protecting the confidentiality, integrity, and availability of information provide a starting basis for security. However, prevention and basic "cyber hygiene" are not adequate to protect against state threat actors and modern attacks. An Adaptive Defense is a security posture that effectively applies an intelligence and risk-based approach to cybersecurity. Because cyberattacks are inevitable, emphasizing detection rather than prevention will promote more effective security. This approach accepts that the organization may "lose" at the tactical level and be breached; however, quick detection and response will prevent serious harm.

3. Response: Remediation support and the ability to quickly recover from an attack are the essence of an Adaptive Defense. Response should include both the capability to recover quickly from cyberattack and a measurement of the time necessary to resume critical operations after an attack. Response should also include the following sub-domain controls:

- Incident management
- Service continuity management (has a strong dependency on asset identification and management)
- External dependency management
- Internal and external communication
- Stakeholder management

The Response Strategy must among other things establish an incident response coordinator and define protocols that efficiently and effectively inform key stakeholders. These protocols should govern privacy disclosure requirements and assignment of work streams for investigation, remediation, communication, and execution of the response plan.

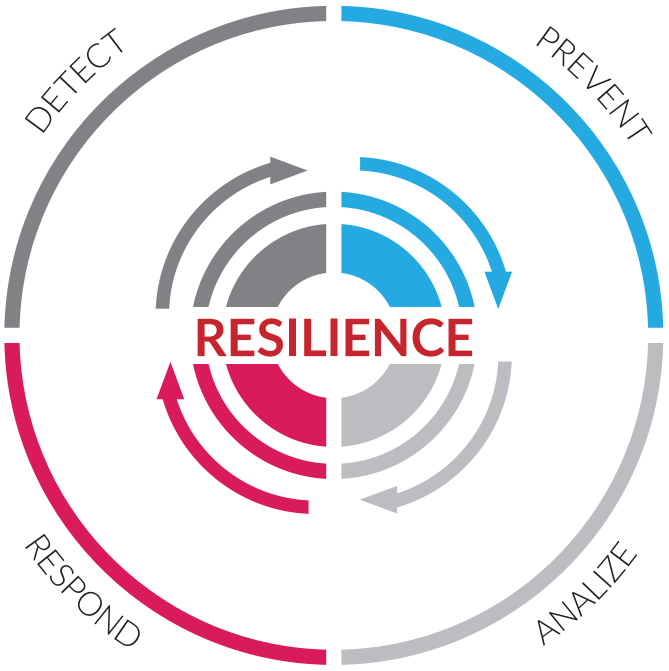
> “ At the heart of the Adaptive Defense is the concept of continuous improvement.

Finally, analysis of “lessons learned” from each attack and response is an important element to guide and adjust intelligence for future responses. Resilience includes learning capabilities. At the heart of the Adaptive Defense is the concept of continuous improvement. This is essential to meet the challenges of emerging and evolving threats. Law enforcement and intelligence services can also be an important partner in effective resilience building.

4. Analysis: Analysis includes containment, forensic investigation and kill chain reconstruction. An effective strategy should emphasize adaptation based on analysis of known attacks. This post-incident analysis forms the basis of an adaptive response by adjusting controls based upon actual known risks. Analysis of known attacks can promote adoption of appropriate technical and organizational measures to safeguard data, systems, and other assets at a security level appropriate to actual risks. This focuses resources on preventing, detecting, and minimizing the impact of known threat methodologies.

Understanding attacker tactics and methods promotes informed decision making, (improved) integration of intelligence, and timely response. Strategic and tactical analysis play an important role in forecasting trends, developments, capabilities, and intentions of attackers, further improving an organization’s Adaptive Defense capabilities.

Figure 1. Illustration of the core elements of Resilience. Source: own compilation.



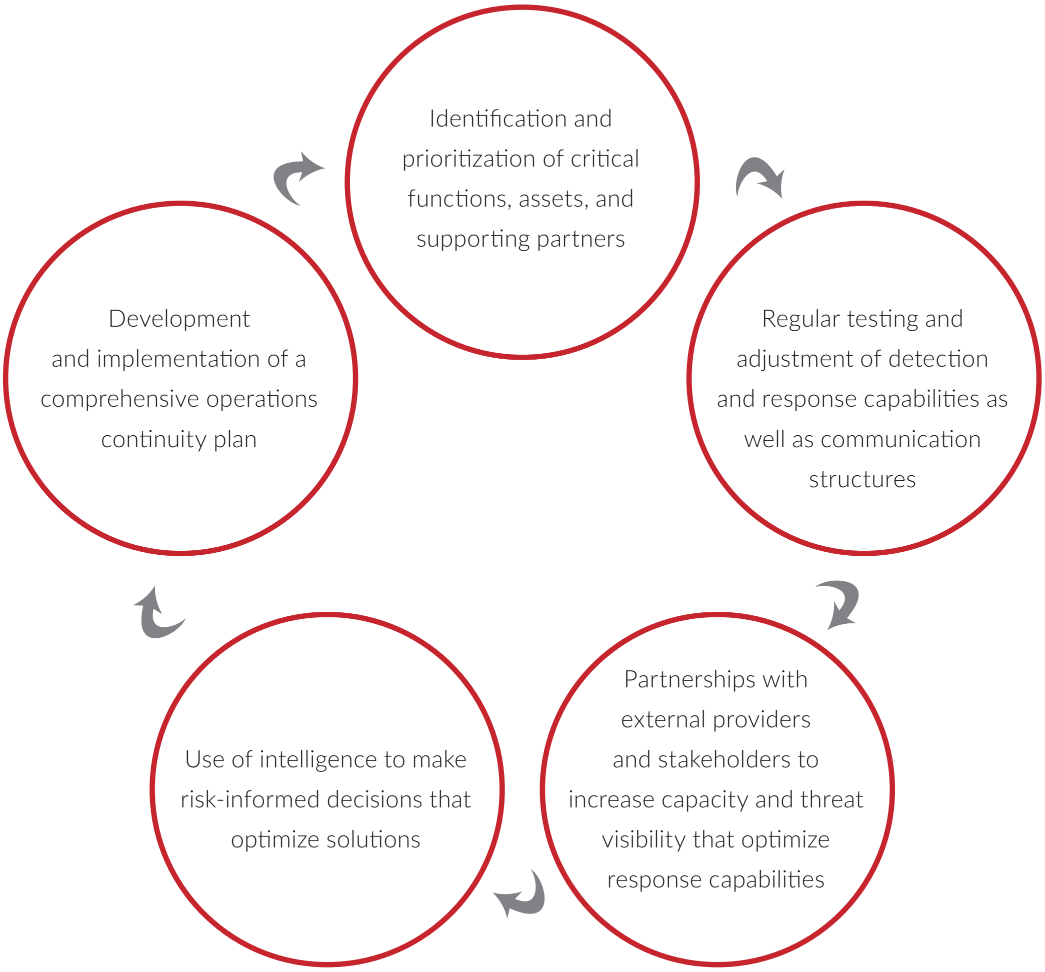
B. Coordination

Adaptive Defense and its main domains should have preventive, reactive, and proactive dimensions. Coordination includes strategies, policies, and activities that further the efficient and effective operation of the cybersecurity strategy across an organization as well as the engagement with external partners.

Strengthened communication between government agencies in cybersecurity matters, between law enforcement and private sector organizations, and between nations plays a central role in increasing the efficiency and effectiveness of responses against cyberattacks.

A foundation for a coordination strategy should include five core areas, as illustrated in Figure 2.

Figure 2. Five areas of action of an Adaptive Defense's coordination strategy. Source: own compilation.


Identification and prioritization of critical functions, assets, and supporting partners
Regular testing and adjustment of detection and response capabilities as well as communication structures
Partnerships with external providers and stakeholders to increase capacity and threat visibility that optimize response capabilities
Use of intelligence to make risk-informed decisions that optimize solutions
Development and implementation of a comprehensive operations continuity plan

Oversight of the coordination process should be a cross-team collaborative approach led by the organizational Chief Information Security Officer (CISO). Security requires a coordination structure to serve as the support mechanism to guide the program, resolve critical decisions, and establish communication channels. Having cross-functional support greatly helps in developing policy and the organizational changes required to be successful.

C. Capacity

A critical element of capacity building is the ability to incorporate (global) threat intelligence or actionable information into an overall organizational adaptive defense. Given the variety and complexity of information sharing needs, it is impossible to identify a single best threat intelligence sharing model. However, key elements should be standardization, harmonization, and appropriate aggregation as well as strategic, tactical, and operational capacities to perform analytical tasks based on threat information. Despite the difficulty of coordinating information sharing between the public and private sectors, exchange of information is critical to building capacity across organizations. The ability to use threat information to identify threat indicators saves time, money and quickens response. This is the foundation of establishing and increasing capacity. Coordination and education are also key elements in establishing and ensuring capacity and cyber resilience. The capacity-building process should identify measures and best practices in support of the core Adaptive Defense domains.

The goal is to adopt a capacity-building approach that leverages internal and external resources to increase organizational capability and facilitate organizational resilience. A critical foundation is to incorporate threat intelligence and incident response planning.

D. Cooperation

The area of public-private partnership, including cooperation with industry partners, the financial sector, academia, and law enforcement, plays an important role in increasing cybersecurity and resilience through raising awareness of threats and preparing adequate support for an effective response. The main areas are:

- Law enforcement partnership (including reporting, prevention, deterrence, disruption, investigation, and victim support)
- Cooperation with third parties, including industry (examples are awareness campaigns, promoting security by design, security by default and privacy by default, and tool development)
- Communication channels for the secure and lawful exchange of information and intelligence with relevant partners

When it comes to detecting and preventing cyberattacks the cliché “it takes a network to defeat a network” is often used. Given the borderless, asymmetric character, volume, level of sophistication, and financial impact of these attacks, cooperation of all stakeholders at national and international levels is key to an Adaptive Defense. This also needs standardised rules of engagement, as well as a clear understanding of the extent to which private parties can obtain evidence themselves and the legal implications of their actions.

CONCLUSION

An Adaptive Defense effectively applies all of the core security domains at a level appropriate to the threats and risk posture of the organization and adjusts strategic decisions based on real-time, global, actionable intelligence. The CMM model provides a framework for evaluating and implementing an Adaptive Defense plan. The CMM process can help create an increased understanding of existing capabilities and an accurate assessment of needs. This provides greater awareness of risks and improves the security readiness process. The development of an information security maturity model requires long-term planning and internal support. It is critical to adopt measures that incorporate emerging best practices into a security framework that will place the organization in a better position to detect and defend against sophisticated cybersecurity threats. An Adaptive Defense is the intended outcome of the CMM process. It is an efficient and effective long-term holistic response to cyber threats. This includes coordinating mechanisms, intelligence sharing systems, and effective policy frameworks leading to a sustainable, agile, and effective risk management security programme.