Chapter 5

Implementing a Defense-in-Depth Strategy

At this point in the journey it is time for you to define the methods by which you will defend your organization's assets and information against cyber adversaries and insiders with malicious intent. The previous chapters have guided you to this point. You have learned how to design your cybersecurity program, define a governance foundation, create an ability to identify threats and vulnerabilities, and assess the risk to your organization. Now it is time for you to do something about it. In this chapter, you will learn how to structure a series of barriers to thwart the advance of bad actors and halt or deter their sophisticated, persistent threat methods. The barriers you select will be based on your organization's risk profile commensurate with the value of your organization's assets and information.

This chapter will help you to:

- Understand the fundamental concepts of defense-in-depth.
- Define defense-in-depth strategies to support your cybersecurity program.
- Look at defense-in-depth as a multi-dimensional strategy.
- Understand available countermeasures to protect assets and information.

5.1 Defense-in-Depth

Defense-in-depth is a concept coined by the US military to describe the placement of defensive barriers to impede the advancement of combatants from overtaking a held position. This military strategy included monitoring the combatants' progress and responding to their advances with equal or greater force. Applying this same concept to the cybersecurity world where threat actors are the combatants and countermeasures are the defensive barriers is perfectly suited to protecting your organization's assets and information. The use of barriers or layers is the foundation of defense-in-depth. Each layer is designed to thwart a type of attack and leverage one another so that if one layer fails to stop an attack, another layer takes over. This strategy is ideal to combat hydra attacks where multiple attack methods are launched against an organization to compromise multiple attack-surface vulnerabilities.

You may have heard defense-in-depth referred to as the *castle* or *onion* approach. Castle analogies are not bad because you can visualize walls, motes, drawbridges, etc. - all varying levels of attack deterrence. The onion analogy is apropos as well as it represents the peeling back of layers of

protection before reaching the bulb, the prized asset. Regardless of the analogy, the concept remains the same - place as many barriers between you and the bad guy. I first started using defense-in-depth strategies in the early 1990s to protect client-server environments, and although the options for layers were limited, they nonetheless worked well because attacks were simpler then.

Today, cyberattacks are more sophisticated and threat vectors more numerous. Defense-in-depth approaches have also become more sophisticated but are still limited by their one-dimensional approach. Stacking layer upon layer like a wedding cake hoping that a cyberattack would pass neatly and sequentially through each layer did not always provide the level of protection necessary. I believe that defense-in-depth is as applicable today as it was when I first included the strategy in my early security designs. However, some fundamental changes in the strategy are required. This chapter is based on my work to develop defense-in-depth, moving it from a onedimensional to a three-dimensional model. The first dimension has always been represented by the attack surface. The second dimension I defined based on the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) consisting of identify, protect, detect, respond, and recover categories. The third dimension is defined by my six cybersecurity architectural domains, discussed later. Figure 5-1 shows the three dimensions of my defense-indepth model.

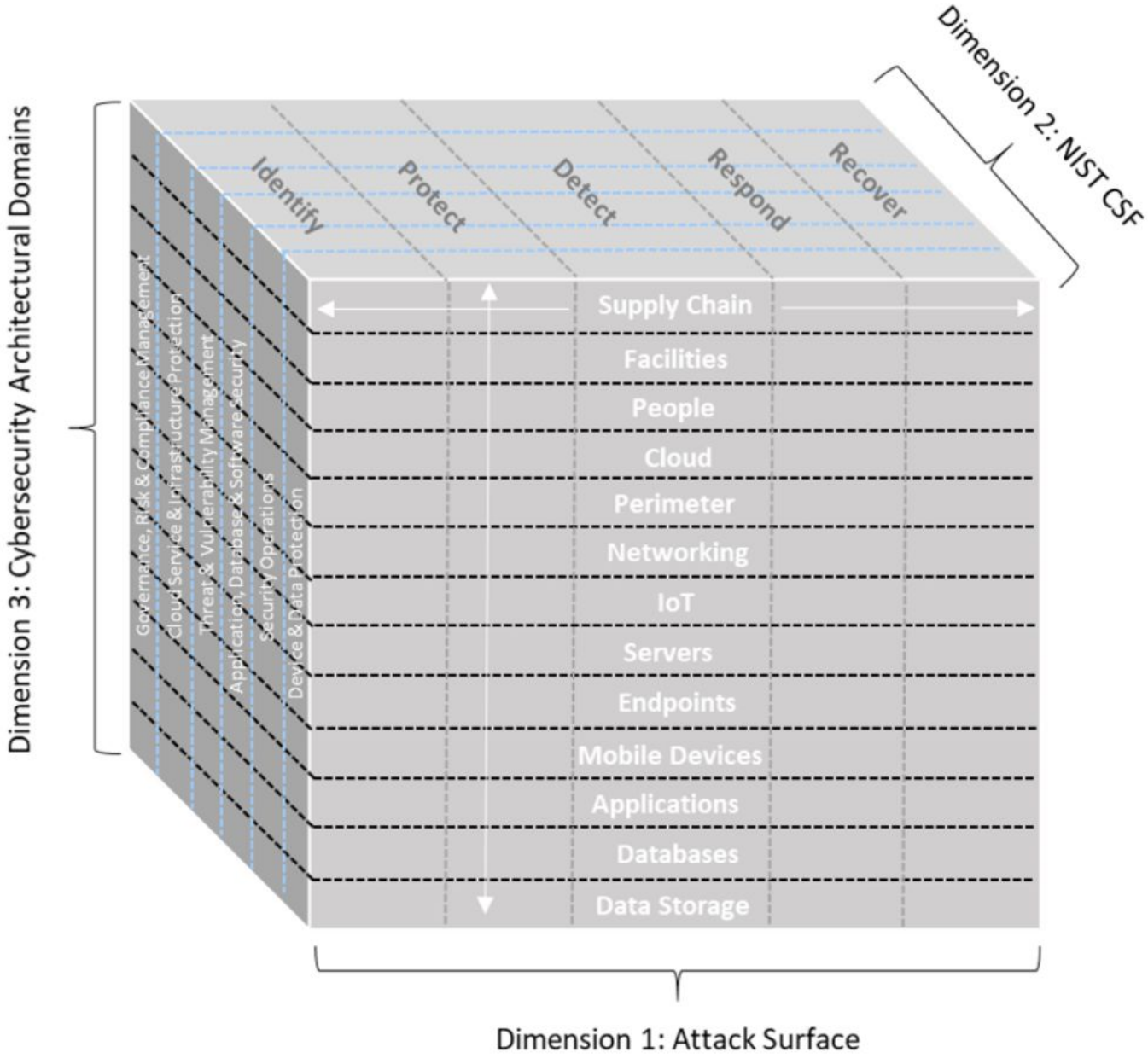

Figure 5-1. Three-Dimensional Defense-in-Depth Model. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

I want you to look at your defense-in-depth from a three-dimensional perspective where you can visualize countermeasures wrapping around as well as cross-sectioning through your attack surface. Once you stop thinking about defense-in-depth as an onion or cake and visualize it as interconnected walls and cross-sections enveloping assets and information like a 360-degree shield of protection you will have taken an important step in outsmarting your adversaries.

> **TIP: Defense-in-depth works best if all the layers integrate and harmonize as one. If you do not interconnect the layers through processes and automation you lessen the effectiveness of the strategy.**

5.1.1 Industry Perception

In April of 2017, I was hosted by the EC-Council to give a speech on defense-in-depth to nearly 700 cybersecurity professionals from over 40 countries. During the session, I asked the audience, "What is your opinion of defense-in-depth?" Table 5-1 shows the results of the response to that question.

Table 5-1. Defense-in-Depth Survey Question

Response	Percentage
It is as valuable now as it ever was.	**90.12%**
Its relevancy is waning.	**6.17%**
Its time has come and gone.	**3.70%**

The clear majority of those attending felt that defense-in-depth was as viable today as it ever was. This is in stark contrast to a myriad of articles I have read over the past several years calling into question the continued usefulness of defense-in-depth. The dichotomy of defense-in-depth is that we as an industry apparently love it but lack proof that it works, so it takes a beating in the press. I was asked not long ago to evaluate a large big box retailer's defense-in-depth strategy. What I found were systemic problems experienced by many organizations' defense-in-depth approaches. First, my client's approach had aged and not kept up with the current threat landscape. Think about all your data residing inside your organization's castle walls. They're nice and safe, right? Now ask yourself, "Will those same walled defenses protect that data when it is moved to the cloud and resides outside the castle walls?"

Another mistake this client made was one I have seen repeated in many other defense-in-depth strategies. This mistake was not addressing the insider threat. Think of your defense-in-depth as a turtle - the outer shell is hard and virtually impenetrable, but turn the turtle over and the soft underbelly is exposed. The threat and vulnerability assessment you learned about in Chapter 3

showed you how to find the soft underbelly of your attack surface. Insider attacks represent the soft underbelly of your organization. You need to act on that knowledge and apply the right countermeasures to protect this exposure point.

5.1.2 Defense-in-Depth Models

Over the years several types of defense-in-depth models have emerged, most assuming basic shapes consisting of circles, squares, pyramids, and even stairs. However, they all had one thing in common - a top down, layered approach to protecting data. Figure 5-2 shows the classic types of defense-in-depth models used today.

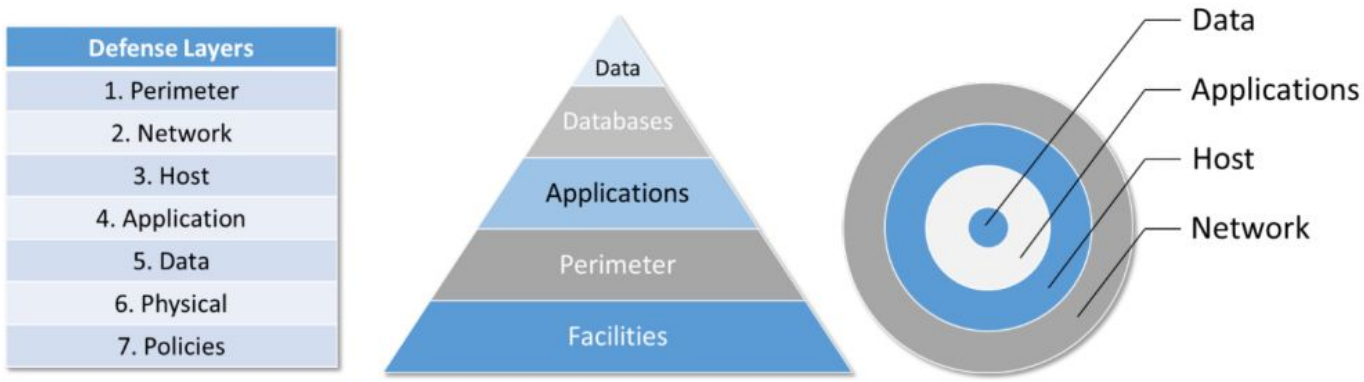

Figure 5-2. Defense-in-Depth Models

During that same EC-Council speech, I asked another question, “What model of defense-indepth is in use?” In response, 57% of those who reported using a defense-in-depth model indicated they use a model based on concentric circles. Table 5-2 shows the results of that survey question.

Table 5-2. Most Used Defense-in-Depth Models

Response	Percentage
Box	**10.10%**
Concentric circles	**40.40%**
None	**30.30%**
Pyramid	**13.13%**
Stairs	**06.06%**

The common denominator of these models is their seeming adoption of defined cybersecurity layers generally modeled after the OSI Model developed by the International Organization for

Standardization (ISO). ISO is the very same organization that brought us many of the security standards we use today (e.g., 27001/27002). The Open System Interconnection (OSI) model is a networking framework with protocols defined in seven layers (applications, presentation, session, transport, network, data link, and physical) (Mitchell, 2016). These layers are used to define the layers of many variations of defense-in-depth. Another approach which, to this day, makes no sense to me is that some security practitioners used the standards of ISO 27001 or NIST 800-53 to define the layers of defense-in-depth. This was wasted effort, since all that is accomplished by this approach is simply to restate what was already defined by ISO or NIST.

Different models had different floors, ceilings, and number of layers, but many began with policies and ended with physical security. Layers ranged from 4 to 10 or more. Regardless of the shape, each model provided a way to visualize how cybersecurity countermeasures related to one another. My goal in this chapter is to show you a new visual approach to defense-in-depth that I believe includes the best of existing models without their shortcomings.

5.1.3 Origin of Contemporary Defense-in-Depth Models

In various models of defense-in-depth I have seen over the years it became clear to me that the majority were based in some part on ISO 7498-2:1989 Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. ISO 7498-2 was introduced by ISO to align their OSI model to mainstream thinking regarding the application of security from an architectural perspective. Even though the ISO 7498-2:1989 model provided little in the way of concrete recommendations, it did offer a formalization of defense-in-depth upon which many models and approaches were later based.

The most important aspect of the ISO security model is that the higher up you go in the security stack, the less you will need to rely on lower-level countermeasures. For years, many organizations have invested the majority of their efforts and investment in countermeasures in the network layer. The thought was to create a strong outer shell. However, as threat vectors changed and the perimeter of an organization became less defined with the advent of mobile computing, this approach proved fallible. A practical example of this would be email security. Email security lives in the application layer of the OSI security model. If you deploy a sound approach to email security in the application layer where email is encrypted and digitally signed, you can be less concerned with the security measures deployed within the network. If you were primarily focusing on protecting the network, your email remained vulnerable. By moving countermeasures close to the attack target, in this case email, you can receive email over an untrusted network and your mail will still be protected. Table 5-3 presents the ISO 7498:1989 security model aligned with the OSI layers with example countermeasures.

Table 5-3. OSI Security Model with Countermeasures Examples

OSI Layer		ISO 7498-2 Security Model	Example Countermeasures
7. Application		**Authentication**	• **Directory security** • **Email security** • **Host firewall** • **Secure browser**

			• Secure coding • Secure file transfer protocol (FTP) • Secure printing
6. Presentation	Logical – Software Oriented	Access control	• Data encryption • Identity and access management (IDAM) • Message encryption • Secure coding
5. Session		Non-repudiation	• Message non-repudiation • Password encryption • Remote login security • Session expiration • Token management
4. Transport		Data integrity	• Firewalls • Port restriction • Session security
3. Network		Confidentiality	• Access control list (ACL) • Firewalls • IPsec • Network intrusion detection system (NIDS) • Malicious packet inspection

	Physical – Hardware Oriented		• Network routing protection • Secure domain name service (DNS)
2. Data link		Assurance/Availability	• Firewalls • Media address control (MAC address) filtering • Wireless security
1. Physical		Notarization/Signature	• Biometric authentication • Data storage encryption • Electromagnetic shielding

5.1.4 Defense-in-Depth Layer Categorization

I am often asked which layer of defense-in-depth is the most important. There was a time that I could easily answer that question, but considering the diversity of cyberattacks, insider threat, and third-party originating compromises the answer has gotten complicated. To answer specifically for an organization, I would need to know its risk profile. However, there is no way I can know the risk profile of all my readers. Regardless, I feel you are owed an answer and I will share with you my thought process that hopefully provides you with the answer you seek.

I follow two general rules when designing a defense-in-depth strategy for my clients. First, the layers nearest to the data are the most important. For example, if you encrypt all your data and secure the encryption keys, several layers can fail and the sensitive information remains secure. Second, not all layers should have the same goal. For example, I design layers to deceive attackers (such as deploying cyber deception), to meet hackers head-on using threat hunting, or to slow them down with firewalls. I have found using the NIST cybersecurity framework effective in defining the second dimension of my defense-in-depth model Table 5-4 explains the use of NIST CSF in dimension 2 of my defense-in-depth model.

In 1998, the National Security Agency (NSA) published an excellent guide that addresses defense-in-depth, the Information Assurance Technical Framework (IATF). The current unclassified version of the IATF is 3.1, published in 2002. Although dated, this framework stands the test of time in its articulation of the concepts of defense-in-depth.

In Chapter 2, I discussed the COSO control framework, which provides great direction and explanation on how to layer compensating controls. I encourage you to review this framework for ideas on structuring or refining your defense-in-depth approach.

Table 5-4. NIST-Based Defensive Layer Strategy

Defense Strategy	Overview
Identify	**Understand the risk of a cyberattack to personnel and assets.**
Protect	**Stop or contain the impact of a cyberattack through manual intervention or automated processes.**
Detect	**Detect attacks before they have an opportunity to achieve successful impact velocity.**
Respond	**Respond to cyberattacks with countermeasures that manage or mitigate their effects.**
Recover	**Stand up to cyberattacks and recover from their aftereffects.**

Next, align your layers to the types of attacks your organization is likely to experience. Which is to say all of them. No organization is immune to any type of attack, so you must assume they all can affect you. Table 5-5 is a model I use as a design guide in aligning countermeasures to attack classes. The countermeasures presented are a small sample of options to counteract the attack classes.

Table 5-5. Attack Class Countermeasures Model

Attack Class	Summary	Example Countermeasures
Active	**An attacker attempting to break into a system by introducing or changing data.**	· **Distribute denial of service (DDoS) prevention** · **Digital signatures** · **Firewalls** · **Intrusion prevention systems (IPS)**
Close-in	**An attack where the adversary has direct or near physical access to the target.**	· **Passwords, session timeouts** · **Physical security** · **Physical surveillance systems**

Distribution	**The utilization of a purposefully programmed hardware or software backdoor that attackers exploit.**	· **Application security scanning** · **Default password prohibition** · **Security testing** · **Trusted hardware/software providers**
Insider	**A trusted insider with access stealing, altering, or damaging information.**	· **Access monitoring** · **Data loss prevention (DLP)** · **File auditing** · **Privileged account monitoring**
Passive	**The secret monitoring or scanning of a network for open ports and vulnerabilities.**	· **Message cloaking** · **Network layer encryption** · **Patch management**
Social	**The use of deceptive social interaction to gain access to systems.**	· **Impersonation fraud detection** · **Security awareness training** · **Social engineering testing**

TIP: Deploy a minimum of three NIST CSF-based countermeasures between the adversary and your data for each attack class. At a minimum, these would include one for detection, one for protection, and one for response. Each countermeasure should present a unique strategy or obstacle to attackers.

Each year dozens of data breach reports are published. I have provided links to the ones I find the most interesting in Appendix A. The information published in these reports can provide valuable insight on how to structure your layers of defense-in-depth. Table 5-6 shows research from Gemalto's Breach Level Index that provides an example of how to align countermeasures based on the most common types of cyber incidents (Gemalto, 2016, p. 6).

Table 5-6. Defense-in-Depth Layer Attack History

Incident Type	%	Attack Class	Countermeasures Strategy

Malicious outsider	**68%**	**Active**	**Countermeasures around intrusion detection, advanced persistent threat (APT) detection, threat hunting, etc.**
Accidental loss	**19%**	**Close-in**	**Countermeasures that encrypt data, improve data handling security and disposal, track lost or stolen devices, and raise the awareness of users.**
Malicious insider	**9%**	**Insider**	**Countermeasures involving access control monitoring and auditing as well as data loss prevention (DLP) and secure data enclaves.**
Hacktivist	**3%**	**Active**	**Countermeasures based on threat intelligence, web damage reversal, DDoS mitigation, and IP blocking.**
State sponsored	**1%**	**Active**	**Measures based on threat intelligence, intrusion detection, advance persistent threat (APT) detection, IP blocking, threat hunting, etc.**

Knowing the percentage of attacks by incident type is important, but I caution you not to rely exclusively on this to drive your defense-in-depth approach. For example, if you place all your efforts in protecting against a malicious outsider and pay little attention to protecting the data you will leave large gaps in your strategy.

5.1.5 Defense-in-Depth Criticism

Defense-in-depth is not without its detractors. Some will argue that you need look no further than the rising success of cyberattacks as proof that defense-in-depth does not work. My take on this criticism is that defense-in-depth gets a bad rap mostly due to the strategy being misapplied. We need to consider that cyberattacks have become more sophisticated and that threat actors are now exploiting threat vectors that typically have never been part of defense-in-depth. These vectors include third-parties, social engineering, and mobile devices. I have also found in my own practice that few of my clients have documented their defense-in-depth strategy. They can certainly show me a picture of a circle, square, or pyramid but not a comprehensive diagram supported by countermeasures mapping. My hypothesis is that many organizations use defense-in-depth in name only. Without detailed analysis of which layer of defense-in-depth was compromised it is difficult to say with any certainty whether a defense-in-depth strategy is to blame. I believe defense-in-depth is not to blame.

There is only anecdotal research on the depth and breadth required for each layer of defense-indepth. We as an industry lack actionable data on the percentage of attacks occurring at each layer. This data would be crucial in determining the appropriate level of investment for each layer, especially given that organizations with finite budgets and a shortage of cybersecurity staff face an adversary with seemingly unlimited resources and methods of attack. I am of the strong opinion that we have failed

defense-in-depth rather than that defense-in-depth has failed us. This can all change and you can reap the benefits of defense-in-depth as it was always intended if you apply defense-in-depth properly. This would include structuring your strategy around:

1. Attack surface layers.
2. Defensive layers.
3. NIST CSF layers.

5.1.6 Defensive Layers

In my three-dimensional defense-in-depth model I define six domains that serve as defensive layers. Each of these domains is discussed in detail later; however, as a precursor to how the defense-in-depth works, I have provided a schema in Figure 5-3 to show their relationship to the other dimensions.

Defense-in-Depth Schema			NIST CSF (Dimension 2)				
Attack Surface Layers (Dimension 1)		**Defensive Layer (Domain) (Dimension 3)**	Identify	Protect	Detect	Respond	Recover
01. Supply Chain	Threat & Vulnerability Management (TVM)	Governance, Risk & Compliance (GRC) Management	●	●	●	●	●
02. Facilities		Governance, Risk & Compliance (GRC) Management	●	●	●	●	●
03. People		Governance, Risk & Compliance (GRC) Management	●	●	●	●	●
04. Cloud		Cloud Service & Infrastructure (CSP) Protection	●	●	●	●	●
05. Perimeter		Security Operations (SecOps) Management	●	●	●	●	●
06. Networking							
07. IoT Devices		Device & Data Protection (DDP)	●	●	●	●	●
08. Servers							
09. Endpoint Devices							
10. Mobile Devices							
11. Applications		Application, Database & Software Protection (ADS)	●	●	●	●	●
12. Databases							
13. Data Storage		Device & Data Protection (DDP)	●	●	●	●	●

Figure 5-3. Three-Dimensional Defense-in-Depth Schema. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

5.2 Improving the Effectiveness of Defense-in-Depth

Now that we have a sound structure for your defense-in-depth approach, a three-dimensional model, how can we make it more effective? I have learned that what is defined within the defense-in-depth model is as important as its skeletal structure. Improving the effectiveness of defense-in-depth comes from embedding countermeasures. Countermeasures, however, need to be properly aligned to each

layer to maximize their ability to manage or mitigate the impact of a cyberattack. To accomplish this, you will need to stop viewing countermeasures as something that resides in a layer, but view countermeasures from a relationship perspective. You will need to answer the question, “What is the relationship of one countermeasure to another?” I have found that grouping countermeasures according to their ability to protect assets and information as well as considering the support they require to operate efficiently is the most effective approach. This may prove to be a difficult proposition to some organizations as they tend to align countermeasures by people. For example, firewalls are an integral part of the network, and with most of them taking the form of an appliance, they are not much different than a router or switch and should belong to the networking department.

To ensure I grouped countermeasures properly, I turned to something called entity relationship modeling. Entity relationship modeling was originally developed for database design by Peter Chen and published in *ACM Transactions on Database Systems (TODS)* (Chen, 1976). I found that entity relationship modeling worked perfectly to describe the inter-relations of countermeasures or controls within defense-in-depth layers. This relationship approach groups countermeasures and controls according to their ability to protect assets and information versus protecting them from specific threats or causes. This is the cause-and-effect notion where you focus on the effect, and not the cause. The old way of protecting against threats required that you layer your countermeasures and controls in anticipation of a cyberattack (cause) progressing through the various layers of defense. The relationship approach aligns countermeasures and controls according to their relationship with assets and information protecting the functions (effects) of the assets and information. There is no assumed primary attack vector for a cyberattack; the assumption is an attack can come from inside or out from any vector and will ultimately reach the intended target. Attacks tend to change the behavior of an asset or its functionality making it violate its own design principle or security policy. For example, a function of email is to allow files to be attached and sent with a message. Changing the email function of file attachments to allow malicious payload attachments is what certain malware accomplishes. So, if you worry less about how the attackers got to the email system and more on what they can change, you will have a higher degree of success in protecting your organization from cyberattacks.

Now what does all this mean? When a cyberattack occurs the objective is to change the behavior of a function of a target. Focusing on layering defenses to stop or slow down the cyberattack at the vector level has proven unsuccessful. The proof of this is offered each time you read about an organization that had a data breach yet complied with all security standards. The organization’s failing was focusing exclusively on protecting the vectors and not the target. For example, there are many vectors that can be used to gain access to data, and history has proven attackers are like the Royal Canadian Mounties - they always get their data. If we assume this is correct, then why not protect the data? If we focused more on encrypting all the data, then protecting the vectors becomes less important. Also, from a cost perspective, I know as a cybersecurity architect that it is far more expensive trying to protect every vector than encrypting all my data.

This is not to say that we completely ignore protecting vectors; it is to say that we spend less on the vectors and more on the target. Another example is in securing the configuration of assets. Attackers want to change the configuration of an asset so they can control its functions. If we apply file integrity monitoring and automatically reverse any file changes any time malicious file changes are detected, we stop the attack.

Figure 5-3 presents the view of this new defense-in-depth model that I have been developing over the past 10 years. It is important to note that this is not an organizational construct for a cybersecurity program; rather, it is how you structure your defense-in-depth strategy. There may be some similarities in defense-in-depth layers and cybersecurity organization layers; however, that is only coincidence. Countermeasure modeling is based on the concept of entity relationship modeling. Figure 5-4 is a countermeasure relationship model I created following the entity relationship model.

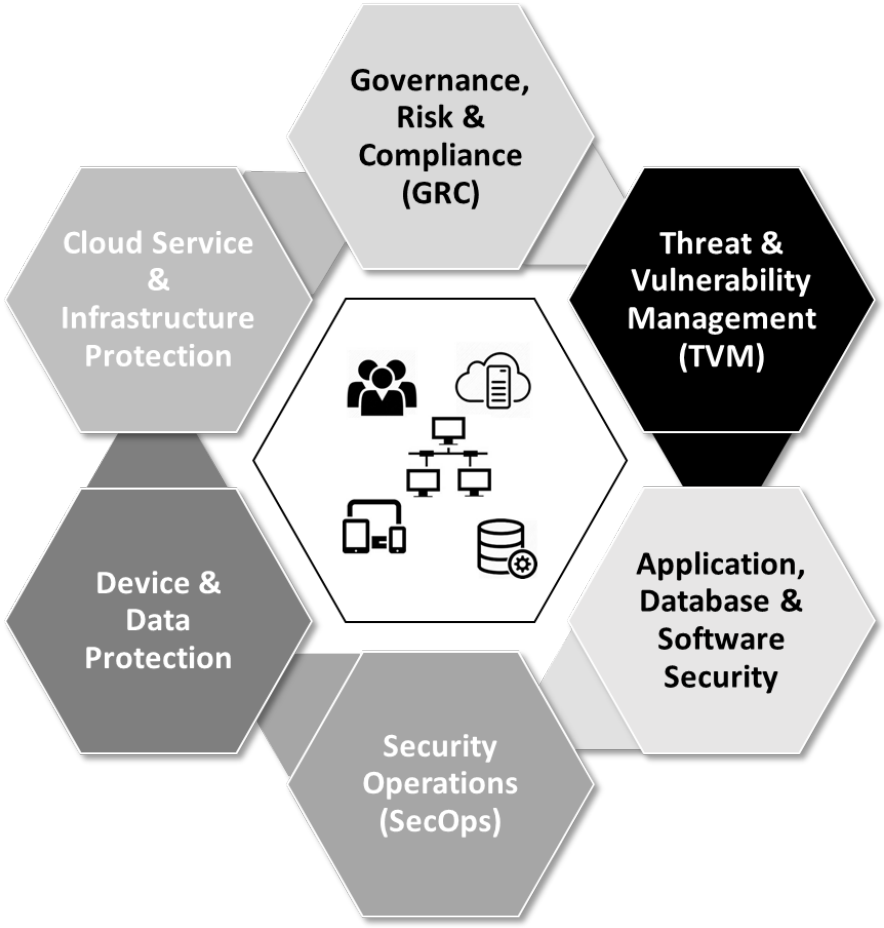

Figure 5-4. Countermeasures Relationship Model. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

This view shows the six domains of the third dimension of the defense-in-depth model. Each domain has been further segmented into subdomains and primary components that were arrived at through the process of entity relationship modeling. The domains of this defense-in-depth strategy cover the full spectrum of a cybersecurity program.

5.2.1 Governance, Risk and, Compliance (GRC) Domain

This subdimension of the model is involved with the overall management of the cybersecurity program from ensuring the proper risk profile is used to base decisions of what countermeasures to use, to managing the budget and allocating the proper resources to staff the program. This subdimension covers many of the functions of the office of the chief information security officer

(CISO). Figure 5-5 represents the structure of the GRC domain. Table 5-7 presents the subdomains and primary components.

Figure 5-5. Governance, Risk, and Compliance Domain. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

Table 5-7. Governance, Risk, and Compliance (GRC) Domain

Subdomain	Primary Components
Strategic planning – Direction and strategy of the cybersecurity program.	· **Body of knowledge (BOK) – Central repository of all documentation, internal and external, used to design and operate the cybersecurity program.**

	· **Cybersecurity program playbook – A quick guide or brochure that describes in layman's terms the scope, objectives, functions, and capabilities of the cybersecurity program.** · **Methods and practices – Documentation of the procedures, processes, and practices used within the cybersecurity program.** · **Program maturity assessment and planning – Baseline security assessment identifying the current maturity of the cybersecurity program. Includes a service improvement plan on how to improve the maturity of all or portions of the cybersecurity program.** · **Security architecture and design – Compilation of all design documents used to develop the cybersecurity program. Includes frameworks, models, standards, blueprints, etc.** · **Security service catalog – Catalog of each of the countermeasures deployed within the cybersecurity program. Describes countermeasures as a service including features, support, and cost.** · **Strategic roadmap – A plan of how the cybersecurity program will evolve over time, reaching strategic objectives consisting of scope, capabilities, investment, reduction of risk profile, etc.**
Cybersecurity governance – Overall management of the cybersecurity program and personnel.	· **Budget management – Manage the capital expenditure (CapEx) and operating expense (OpEx) of the cybersecurity program finances. Justify that expenses are commensurate with value of assets at risk and annualized loss expectancy (ALE).** · **Cybersecurity metrics registry – Repository of all cybersecurity program key performance measures and metrics with cross-mapping of metrics to provide an operational effectiveness view by program components.** · **Cybersecurity personnel management – Ensure proper staffing and assignment of roles and responsibilities. Overview cybersecurity skills certifications and training.** · **Cybersecurity project management office – Manage projects directly related to the cybersecurity program and monitor projects indirectly related to the program.** · **Cybersecurity policies – Write and revise cybersecurity program policies, stipulating acceptable use of assets and information and articulating the principles of protecting the**

	organization from cyberattack.
Compliance – Compliance with legal, regulatory, and contractual requirements.	· **Audit response – Manage the internal and external cybersecurity or related regulatory audit process including remediation and tracking of audit citations.** · **Cybersecurity awareness and culture – Maintain a cybersecurity aware culture through an awareness program consisting of training, reminders, and simulations.** · **Cybersecurity law program – Maintain a library of legal and regulatory statutes as well as requirements of compliance.** · **Cybersecurity program performance dashboard – Provide transparent reporting of the performance of the cybersecurity program leveraging the metrics registry.** · **Regulatory compliance assessments and reporting – Annually perform regulatory compliance assessments to determine degree of compliance with privacy and cybersecurity statutes.**
Risk management – Determination and treatment of risk.	· **Risk assessment program – Perform risk assessments of projects, applications, or systems that could introduce risk to the organization.** · **Risk treatment plans – Create approaches to reduce or eliminate risk identified from risk assessments. Monitor and report on risk treatment progress.** · **Cybersecurity controls catalog – Maintain a catalog of compensating controls that are used to treat risk.** · **Red teaming – Perform independent cyberattack simulations against current countermeasures assuming the role of a threat actor.** · **Risk monitoring – Monitor the state of risk to the organization considering changes in asset and information state.** · **Risk reporting – Report on organization risk profile as well as the risk posture of applications, projects, and systems. Integrate Third-party risk reporting in overall risk profile.**
Third-party management – Validation of cybersecurity policy compliance and risk monitoring.	· **Compliance reporting – Report on third-party supplier compliance with cybersecurity policies and risk profile.** · **Continuity of supply chain – Monitor state of supplier**

	continuity and maintain continuity plans in the event of supplier failure. · **Risk management – Perform periodic risk assessments of third-parties, assign risk scores, and monitor changes to risk scores.** · **Security controls agreement – Maintain current cybersecurity controls agreement with third-parties and monitor and act on compliance violations.**
Business continuity management (BCM) – Resiliency and recovery of technology.	· **Recovery of cybersecurity technology – Make ready and test capability to recover cybersecurity countermeasures in the event of failure.** · **Resiliency of cybersecurity technology – Ensure the continued operations of cybersecurity countermeasures in the event of operational disruption.** · **Recovery of cybersecurity program data – Ensure the recoverability of security logs and security event data.** · **Security of BCM operations – Ensure the security of recovery operations and continuation of asset and information protection.**

5.2.2 Threat and Vulnerability Management (TVM) Domain

This domain is concerned with identification of the threats faced by the attack surface and the vulnerabilities that could be exploited by the threats. The attack surface is continuously monitored for vulnerabilities with noted vulnerabilities remediated to prevent exploitation. The threat landscape is assessed to identify current and emerging threats. Figure 5-6 represents the structure of the TVM domain. Table 5-8 presents the subdomains and primary components.

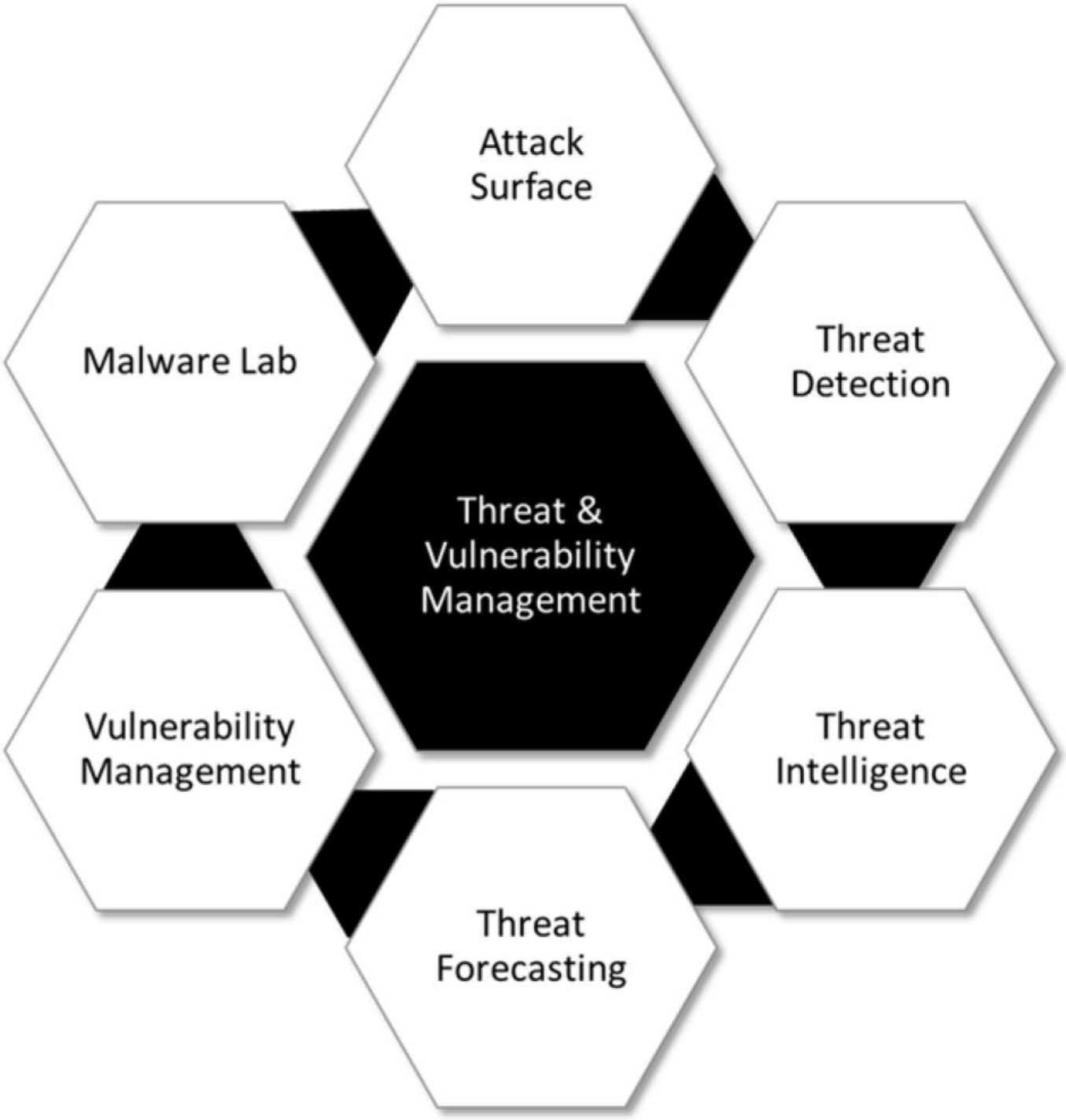

Figure 5-6. Threat and Vulnerability Management Domain. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

Table 5-8. Threat and Vulnerability Management Domain

Subdomain	Primary Components
Attack surface – Inventory and management of an organization's hardware and	· **Device and software inventory – Detailed inventory of computing assets and software. Commonly contained in a configuration management database (CMDB).**

software assets.	· **IT asset discovery – Automated network discovery and tagging of cyber assets connected to the network.** · **Shadow IT discovery – Discovery of unauthorized cloud computing services.** · **Third-party service provider directory – Directory of third-party service providers with detailed company and service descriptions.** · **User population management – Identification and management of network user identities classified by threat class.**
Threat detection – Detection of external and insider attacks.	· **Advanced persistent threat (APT) detection – Series of countermeasures designed to detect the behaviors of an APT attack.** · **Data theft detection – Data loss prevention to detect accidental or intentional data exfiltration.** · **Denial of service (DoS) attack prevention – DoS prevention solution that detects degraded Internet service and counteracts attacks with load balancing and application acceleration.** · **DNS monitoring – Secure DNS security and privilege access control and monitoring.** · **Malware detection and removal – Detection, quarantine, and/or removal of malicious software on servers and endpoints.** · **Threat hunting – Detection of lateral hacker movement inside the network. Techniques to halt hacker activity once detected.**
Threat intelligence – Gathering, analysis, and dissemination of threat intelligence and attacker profiles.	· **Honeynets and honeypots – Faux IT infrastructure with decoy information to attract hackers to waste their time on wrong targets.** · **Information sharing and analysis center (ISAC) – Commercial critical infrastructure section threat intelligence shared by specific industries.** · **Open source intelligence feeds (OSINT) – Intelligence collected from publicly available sources.**

	· **Security information and event management (SIEM) – Security event log collection, aggregation, and analysis to detect malicious activity.** · **Threat intelligence subscriptions – Commercial subscription to threat intelligence gathering and reporting service.**
Threat forecasting – Forecast future and potential threats; issue threat advisories and warnings.	· **Cyber threat gaming – Threat attack simulation exercises in the form of a game.** · **Threat actor profiles – Profile of hackers, hacktivists, or other advisories. Includes overview of techniques, motivations, targets, etc.** · **Threat forecasting – Leveraging threat intelligence to forecast likely attack targets of an organization.** · **Threat modeling – Procedure identifying objectives and vulnerabilities, and then defining countermeasures to prevent attacks.** · **Threat registry – Inventory of analyzed threats aligned to attack surface.**
Vulnerability management – Scanning and remediation of attack surface vulnerabilities.	· **Patch management – Remediation of hardware and software vulnerabilities through vendor patches and firmware updates.** · **Vulnerability remediation testing – Testing of applied vulnerability remediation to verify mitigation of vulnerability.** · **Vulnerability scanning – Automated scanning of internal and external networks to detect attack surface vulnerabilities.**
Malware lab – Dedicated lab for reverse-engineering and study of malware.	· **Malware analysis service – Malware analysis capability either in-house or as a service to evaluate new strains of malware to determine countermeasures.** · **Malware analysis system or sandbox – Reverse-engineering of malware to determine how the malware would act when executed inside an isolated environment.**

5.2.3 Application, Database, and Software Protection (ADS) Domain

This domain ensures all new and legacy code is secure in its development, acquisition, and maintenance, meeting industry-accepted security standards. Countermeasures for in-house

developed, common off the shelf (COTS), and database products meet secure coding standards; any exploitable code is identified and remediated prior to release to production. Figure 5-7 shows the structure of the ADS domain. Table 5-9 presents the subdomains and primary components.

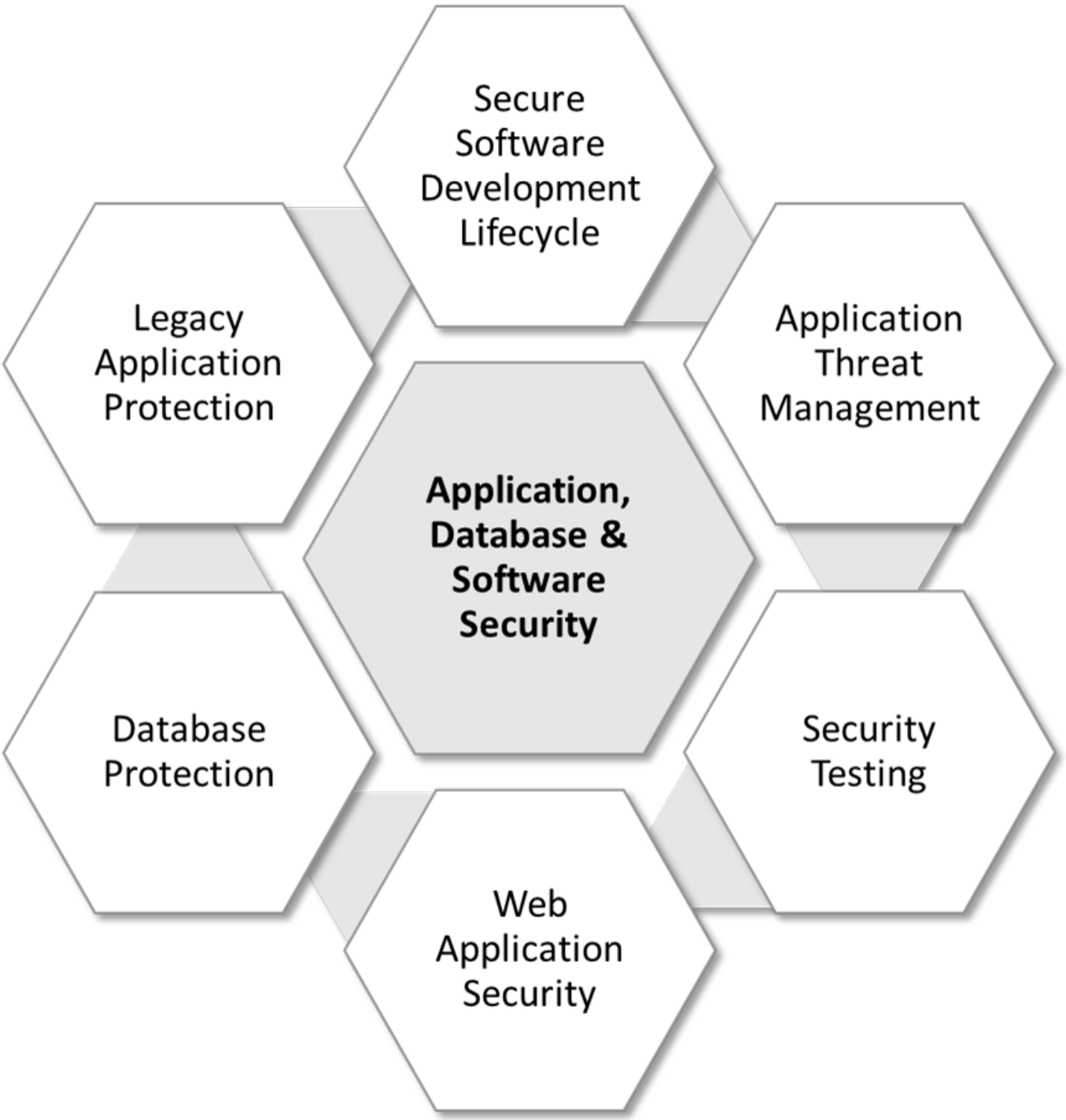

Figure 5-7. Application, Database, and Software Domain. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

Table 5-9. Application, Database, and Software Domain

Subdomain	Primary Components
Secure software development lifecycle – Methods and practices for secure coding standards.	· **Bug tracking – Identifying and tracking application bugs and implementing remediation schedule and plans.** · **Development operations security integration – Integration of security practices to reduce code vulnerabilities in application development.** · **Secure coding policies and practices – Methods and practices of secure coding techniques.** · **Secure programing training – Programmer training in secure coding techniques and good practices.** · **Software composition analysis – Inventory of open source components to identify vulnerabilities, covering open source and commercial code.** · **Source code protection – Secure access and monitoring of source code to prevent introduction of accidental or intentional adverse changes.**
Application threat management – Detection of external and insider application threats.	· **Application patch management – Patching of commercial application vulnerabilities.** · **Application risk profiles – Profile of application's risk and control compliance score.** · **Application security monitoring – Monitoring of application security event log for suspicious activity.** · **Application threat intelligence – Threat intelligence and security vulnerability reporting specific to applications or application code.**
Security testing – Scan applications for vulnerabilities and test for external and internal compromises.	· **Bug bounty program – Program offered to hackers to receive recognition and compensation for reporting bugs, especially those pertaining to exploits and vulnerabilities.** · **Dynamic application security testing (DAST) – The process of testing an application or software product in an operating state.**

	· **Manual code review – Expert firsthand analysis of application code to detect vulnerabilities undetected by automated vulnerability scanning.** · **Penetration testing – External or internal attempt to compromise a network or application using hacker techniques.** · **Static application security testing (SAST) – Set of technologies designed to analyze application source code, byte code, and binaries for coding and design conditions that are indicative of security vulnerabilities.**
Web application security – Protection of web applications.	· **Multi-factor authentication – A method of access control in which a user is granted access only after presenting several separate pieces of evidence to an authentication mechanism.** · **Intrusion prevention system (IPS) – Security device to monitor and log network or system activities for malicious activity and block or stop an attack.** · **Reputation filtering – Mail flow policies based on sender reputation, which prevents malicious traffic from entering a network, allowing legitimate mail to flow unobstructed.** · **Web application firewall (WAF) – Appliance, server plugin, or filter that applies a set of rules to a Hypertext Transfer Protocol (HTTP) conversation to prevent cross-site scripting (XSS) and Structured Query Language (SQL) injection attacks.**
Database protection – Protection of databases and associated data.	· **Database access monitoring – Privileged user and application access monitoring independent of native database logging and audit functions.** · **Database encryption – Transformation of data stored in a database into cipher text that is incomprehensible without first being decrypted.** · **Database vulnerability scanning – Scanning of databases for security vulnerabilities and configuration flaws, including patch levels.**
Legacy application protection – Security and isolation of non-secure legacy	· **COBOL and Fortran source code vulnerability scanning – Legacy code scanning software to detect application vulnerabilities.**

applications.	· **Mainframe access control – Access control solutions such as Resource Access Control Facility (RACF) or Access Control Facility (ACF2).** · **Noncompliant application sandbox – Segmenting or insulating applications with known security vulnerabilities that cannot be remediated into a secure zone.** · **Source code comprehension – Application analysis tool that documents how an application functions when no documentation is available. Used for security analysis of legacy applications.**

5.2.4 Security Operations (SecOps) Domain

This domain handles the day-to-day operations of security countermeasures and controls to protect assets and information. Engineering of cybersecurity solutions to integrate into the organization IT infrastructure and the configuration and maintenance of cybersecurity technology and products occur within this component. The ongoing monitoring of cyberattacks and cyberattack response is driven from this component's big data analytics capability. Figure 58 represents the structure of the SecOps domain. Table 5-10 presents the subdomains and primary components.

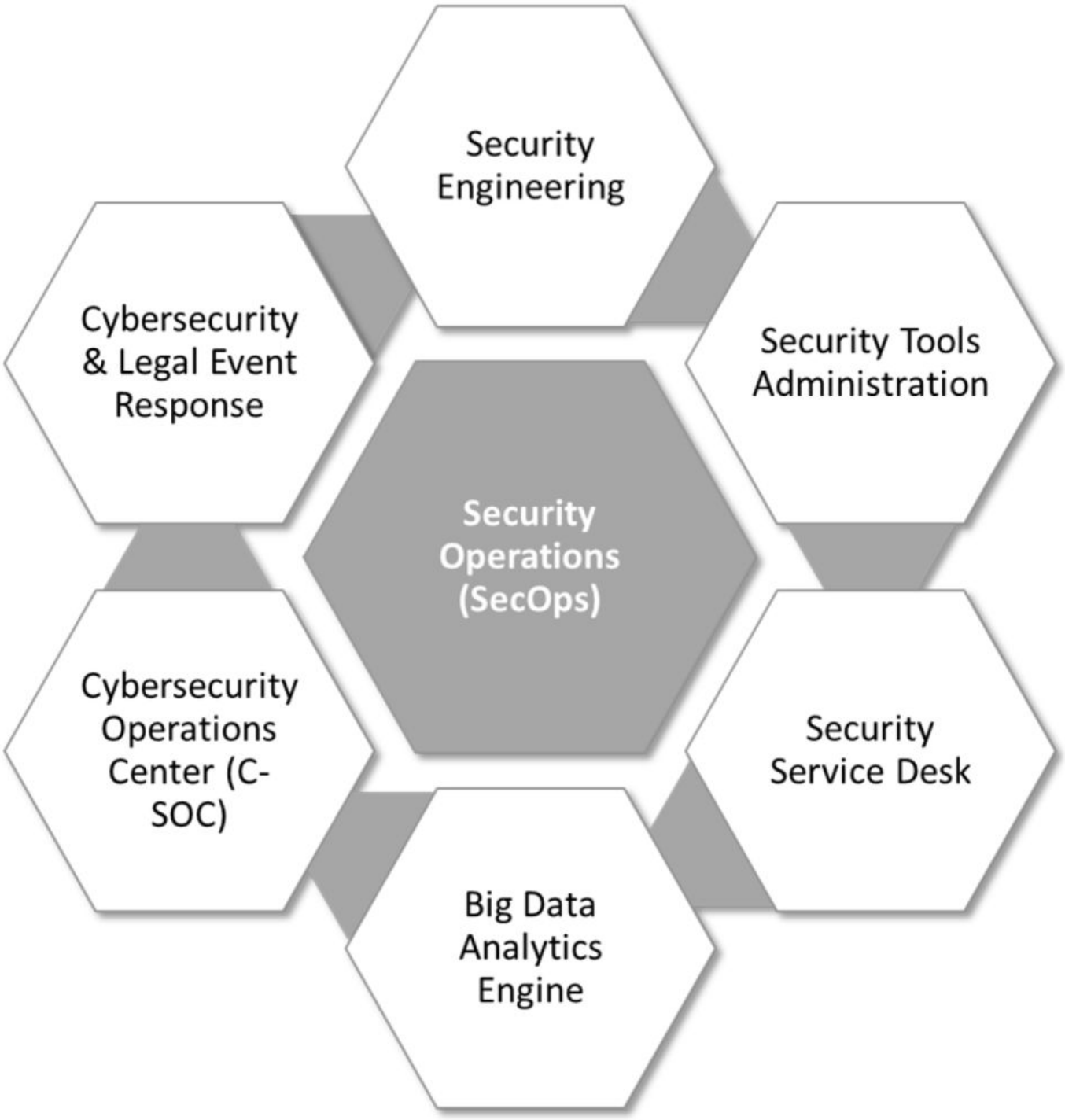

Figure 5-8. Security Operations Domain. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

Table 5-10. Security Operations Domain

Subdomain	Primary Components
Security engineering – Technology engineering consisting of script writing, connectors development, and engineering design.	· **Asset hardening – Restricting open ports and enabled services as well as ensuring current patches are applied to cyber assets.** · **Countermeasures maintenance and testing – Maintain current release and patch levels of cybersecurity technology and test functionality of new releases prior to deployment.** · **Identity and access management (IDAM) Engineering – Write connectors to bridge IDAM technology with authoritative user and provisioning source applications.** · **Network security engineering – Design secure network, establish secure networking practices, and harden network infrastructure devices (e.g., switches and routers).** · **Cybersecurity technology integration – Test and evaluate new cybersecurity technologies to validate integration within current IT environment.**
Security tools administration – Administration and maintenance of cybersecurity technology.	· **Countermeasure administration – Daily operations support of cybersecurity technology and troubleshooting operational issues.** · **Cybersecurity technology updates and deployments – User testing of cybersecurity product enhancements and deployment and training.** · **Firewall and IDS/IPS administration – Application of firewall rules and IDS/IPS signatures following management of change procedures.** · **Proof of concepts – Test new cybersecurity technologies against use cases.** · **Technology health checks – Periodical assessment of the performance and effectiveness of cybersecurity countermeasures.**
Security service desk – Provide user support for	· **Level 1 support countermeasures – First-level support of cybersecurity countermeasures. Diagnose failed reporting,**

cybersecurity program	**broken alert streams, etc.** · **Password resets – Reset user passwords, issue initial passwords, and assist in user access issues.** · **Security incident reports – Security incident and event reporting produced by various cybersecurity program products.** · **Security trouble ticketing – Opening, processing, and closing of security-related user trouble tickets.** · **Token provisioning – Provide or revoke new or replacement two-factor authentication software and hardware tokens.** · **User malware infection remediation – Assist users in resolving localized malware infections.**

technology, user device virus infections, and access administration.	
Big data analytics – Perform advance data analytics using all available security event and intelligence feeds.	· **Big data analytics platform support – Support of big data platform consisting of Hadoop, server clusters, analytic software, etc.** · **Data mining – Advanced analytics using sophisticated threat analysis beyond SIEM analysis.** · **Facilities security feed integration – Integration of closed-circuit television (CCTV), access control, life/safety, and other physical security controls into SIEM and big data analytic platforms.** · **Reporting and analysis – Security event pattern analysis from big data sources.** · **Security feed administration – Maintenance and support of internal, external, and open source data feeds.**
Cybersecurity operations center (C-SOC) – Dedicated security event monitoring and response operation.	· **Alert triage – Analysis and categorization of counsel alerts.** · **Incident response – Response procedures to act on cyberattacks underway.** · **Log analysis – Review and analysis of security event logs to detect suspicious activity.** · **Managed security service provider (MSSP) support – Daily support and shift turnover of MSSP operations.** · **Network operations center (NOC) liaison – Interface with NOC to coordinate NOC and C-SOC alerts.** · **Security event monitoring – 24x7x365 live monitoring of security alerts and indicators of compromise.** · **Threat hunting – Investigation and hunting of underway cyberattacks.**
Cybersecurity and legal event response – Provide incident and legal event support.	· **Cybersecurity insurance – Policy to cover costs associated with a data breach and related lawsuit.** · **Data breach response – Response plan to handle specific data privacy breach regulatory violations.**

	· **Digital evidence gathering – Procedures, practices, and products to gather legally admissible digital evidence.** · **Document discovery support – Production and preservation of court ordered discovery documents.** · **Legal hold support – Issuance and tracking of legal holds of documents requested under court order.** · **Security incident response support – Operations support of incident response plans.**

5.2.5 Device and Data Protection (DDP) Domain

This domain focuses on device and data protection which are inexorably linked. Confidential and sensitive information is managed throughout its lifecycle to ensure the integrity of data creation, secure data movement, and finishing with secure data disposal. Countermeasures for protecting data share common and leveraged approaches, such as device and data encryption. Figure 5-9 shows the structure of the DDP domain. Table 5-11 presents subdomains and primary components.

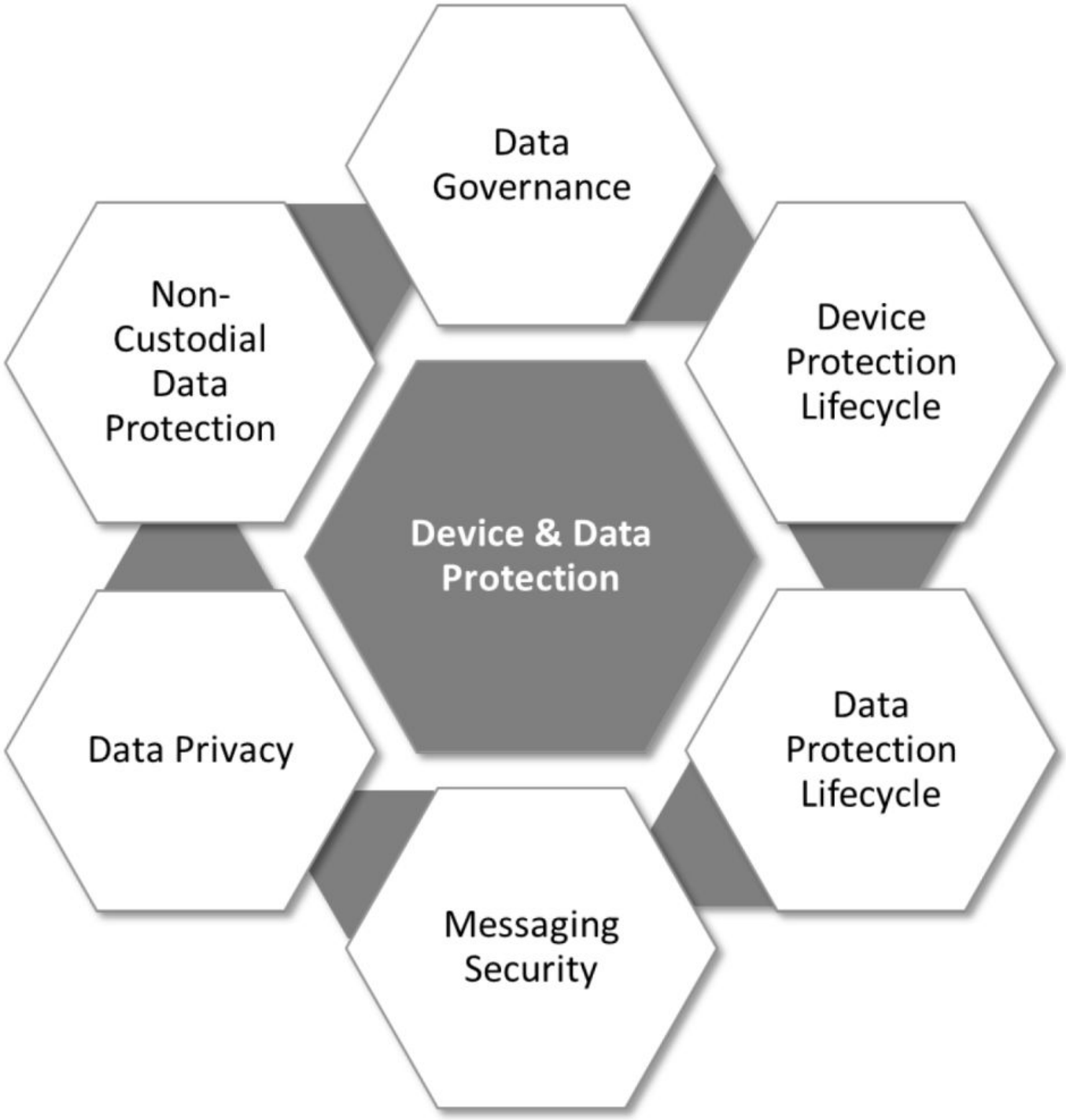

Figure 5-9. Device and Data Protection Domain. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

Table 5-11. Device and Data Protection Domain

Subdomain	Primary Components
Data governance – Definition of data handling requirements and protection of data throughout its lifecycle.	· **Data archiving – Retention of information for an extended period. Generally required by legal or regulatory statutes.** · **Data backup – Duplication of data to allow retrieval of a backup set of data in the event of loss of original data.** · **Data classification – Categorization of data into types or other distinct levels for data management and tracking.** · **Data integrity – Assurance of the accuracy and consistency of data throughout its lifecycle.** · **Data retention – Retaining of information for specific periods of time to meet business and legal requirements.** · **eDiscovery – Electronic discovery of information during litigation investigations.**
Device protection – Methods to prevent devices from compromise and malware infection.	· **Endpoint protection – Integrated cybersecurity solution designed to protect user devices consisting of DLP, firewalls, IDS/IPS, anti-malware, etc.** · **Mobile device security – Protection of smartphones, tablets, laptops, and other portable computing devices from wireless-related threats and vulnerabilities.** · **Server hardening – Reduction of threat vectors through the disabling of services, closing of unnecessary ports, and application of security patches.** · **Server security solutions – Server-specific security measures consisting of connection authentication, service restriction, firewalls, file integrity monitoring, and intrusion detection/prevention.** · **Virtualization security – Protection of the hypervisor layer protecting all virtual machines on the host. Includes anti-virus, IDS/IPS, firewalls, etc.** · **Whitelisting/Blacklisting – Restriction of applications that can and cannot run on cyber devices.**

Data protection – Methods to maintain the privacy of data once stolen.	· **Data anonymization – Removal or changing of record codes or keys to prevent the linking of sensitive data to actual data.** · **Data blurring – Conversion of real data with rounded up data, average of all data, and other techniques to mislead viewer on exact data content.** · **Data camouflage – Replacement of actual sensitive data with fictional data so that the information may be used without violating privacy protections.** · **Data de-identification – Removal of personally identifiable information from datasets.** · **Data encryption – Use of cryptographic techniques where data is rendered unreadable without the presence of a unique encryption key to decode the encrypted data.** · **Data masking – Masking or concealing of sensitive data within a dataset so that the data can be used without revealing privacy-protected information.** · **Data obfuscation – Scrambling of data to prevent unauthorized access to sensitive information.** · **Data perturbation – Small changes to data to prevent identification of individuals from unique or rare data subsets of large populations.** · **Data redaction – Expunging of sensitive information prior to disclosure.**
Messaging security – Maintaining privacy and integrity of messages.	· **Content privacy monitoring – Monitoring of content flow to determine violation of data privacy policies.** · **Data loss prevention (DLP) – Monitoring of content flow within a network or egress points to identify accidental or unauthorized release of sensitive information.** · **Ephemeral messaging – Messages that expire or disappear within a specified period.** · **Message compliance retention – Retention of all forms of messaging that must be retained for legal or regulatory requirements.** · **Messaging encryption – Sending and receiving messages through email, etc. where the recipients must have an**

	encryption key to read and respond to the message. · **Secure messaging – Secure, private methods to facilitate sharing of sensitive information between parties. Messages can be configured to verify receipt, restrict printing or forwarding, etc.**
Content security – Protection of content from alteration, theft, eavesdropping, and loss.	· **Piracy monitoring – Internet scanning to locate and remove copyrighted material.** · **Content encryption – Use of cryptographic techniques where content is rendered unreadable without the presence of a unique encryption key to decode the encrypted content.** · **Data alteration detection – Method to detect the alteration or tampering of information from its original source.** · **Digital rights management (DRM) – Control of the use of digital data restricting its storage, printing, forwarding, and modification.** · **Digital signatures – Authenticated, non-repudiation signature that replaces a wet signature.** · **Email attachment security – Configuration of email attachment functions to validate security policies. Includes attachment interrogation and remediation.** · **Screenshot detection and disablement – Disabling of or detection of someone performing a screenshot within a web browser.**
Non-custodial data protection – Protection of data held or processed by others.	· **Data controller privacy policies – Privacy preserving and information handing policies that direct what a data custodian may or may not do with sensitive information.** · **Data fingerprinting – Adding of unique identifiers to sensitive information to track movement.** · **Digital rights management – Control the use of digital data restricting its storage, printing, forwarding, and modification.** · **Encryption key custody – Retention of the second dual encryption key so that data custodians can comply with court orders without violating organization privacy agreements.**

5.2.6 Cloud Service and Infrastructure Protection (CIP) Domain

This domain addresses the protection of data stored in the cloud, and the security of the cloud services consisting of infrastructure as a service (IaaS), software as a service (SaaS), platform as a service (PaaS), etc. Figure 5-10 presents the structure of the CIP domain. Table 5-12 presents the subdomains and primary components.

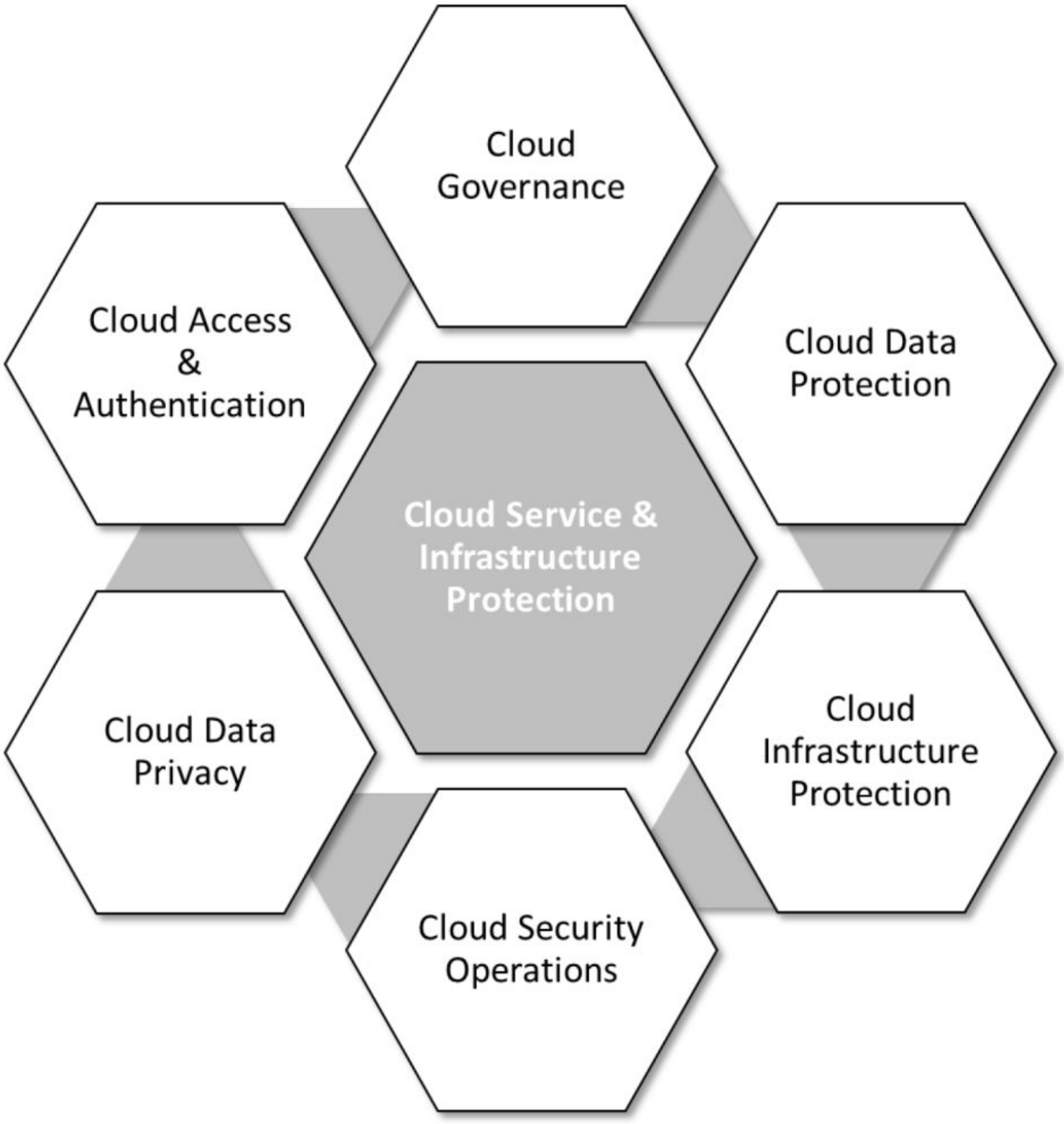

Figure 5-10. Cloud Service and Infrastructure Protection Domain. (By Tari Schreider, licensed under a Creative Commons Attribution-NonCommercial-NoDerivitives 4.0 International License)

Table 5-12. Cloud Service and Infrastructure Protection Domain

Subdomain	Primary Components
Cloud governance – Oversight and control of cloud data and processing.	· Amazon web service (AWS) control compliance monitoring – Monitor control compliance state of AWS security settings. · Cloud access security broker (CASB) – Cloud access security policy enforcement point for access, encryption, malware detection, etc. · Cloud security policy enforcement – Monitoring, reporting, and enforcement of cloud security policies. · Shared responsibility security model – Security model where both parties share in the responsibility to protect cloud assets and information.
Cloud data protection – Protection of data held or processed by cloud service providers.	· Cloud collaboration software – Secure cloud collaboration solution. · Cloud encryption gateways – Cloud security proxy, which provides encryption, tokenization, or both. · Digital rights management – Control the use of digital data shared in the cloud to restrict its storage, printing, forwarding, and modification. · Dual encryption key custody – Two-key process to prevent the disclosure of information by cloud service provider.
Cloud infrastructure protection – Protection of hardware used to deliver cloud services, primarily private and hybrid cloud.	· Cloud server intrusion detection system (IDS) – IDS performed as software as a service (SaaS). · Cloud vulnerability assessment – Scanning of cloud platform for vulnerabilities. · Configuration auditing – Auditing of cloud service provider infrastructure security configurations. · High risk connection intelligence – Monitoring of websites to determine if they have been compromised or hijacked. · Virtualization security and virtual machine hardening – Protection of the hypervisor layer protecting all virtual

	machines on the host. Includes anti-virus, IDS/IPS, firewalls, etc.
Cloud security operations – Ensuring the security of cloud operations and workload processes.	· **Cloud security monitoring – Monitoring cloud service provider or cloud infrastructure security.** · **Cloud server configuration hardening – Hardening of cloud infrastructure.** · **Cloud server misconfiguration detection – Detection and alerting of cloud service provider server or service misconfigurations.** · **Cloud service provider certification validation – Monitoring of cloud service provider security certification status including renewals and revocations.** · **Cloud topology visualization – Cloud topographical diagram showing data path, attack surface, and data residency.** · **Cloud workload security – Could workload visibility to identify security gaps created by unauthorized changes, suspicious behavior, unknown vulnerabilities, and zero-day threat hardening.**
Cloud data privacy – Protection of data residing in or burst in the cloud.	· **Cloud data loss prevention (DLP) – DLP policies extended to data residing in the cloud.** · **Cloud data privacy monitoring – Monitoring of privacy violations of data residing or processed in the cloud.** · **Cloud-based email scanning – Cloud-based email security scanning prior to delivery to enterprise email servers.** · **Data sovereignty policy – Data privacy policies outlining privacy protections for individual countries where customers and/or data reside.** · **Security as a service (SECaaS) – Contracted security services to replace or augment in-house security services.**
Cloud access and authentication – Controlling the access to cloud data or resources.	· **Identity management as a service (IDaaS) – Cloud-based centralized administration and provisioning of user accounts, applications, and devices.** · **Multitenant active directory (AD) hardening – Hardening of AD used for cloud users, accounts, and applications.**

	· **Multitenant active directory (AD) monitoring – Monitoring of AD for unauthorized or suspicious directory changes.** · **Privilege cloud account access monitoring – Monitoring of administrator, service, and shared accounts for abnormal behavior.** · **Time-limited network port and out-of-band (OOB) access control – Assignment of time-bound access to network ports or OOB maintenance and support ports.**

TIP: Check out the Cloud Security Alliance (CSA) Cloud Controls Matrix for additional insight into applicable countermeasures.

It is important to allow countermeasures from one domain dimension to provide services to another domain dimension regardless. For example, vulnerability assessments may reside in the threat and vulnerability management domain of dimension-three, but those services can also be shared by other domains in dimension-three such as cloud service and infrastructure protection.

5.3 Defense-in-Depth Model Schema

To help you with planning and documenting your defense-in-depth model, Table 5-13 provides you with a template you can copy to an Excel spreadsheet. Once you have created your spreadsheet, start adding your attack surface layers, and cross map those to the domains, subdomains, and primary components previously discussed in this chapter. Next, enter the specific countermeasures you will use to enforce or support the primary components. Then use Table 5-4 as a legend to identify which NIST CSF category to align to your countermeasures.

Table 5-13. Defense-in-Depth Model Schema.

Attack Surface	Domain	Subdomain	Primary Components	NIST CSF Category	Countermeasures
Supply chain	GRC	Third-party management	Compliance reporting	Detect	Third-party compliance state reporting dashboard
			Continuity of supply chain	Recover	Supply chain business continuity plan
			Risk management	Identify	Third-party risk assessment
			Security controls agreement	Protect	Third-party cybersecurity controls agreement
			Supplier incident response	Respond	Third-party incident response plan

You should strive to identify countermeasures for each NIST CSF category for each primary component. If you were to do this for each of the primary cybersecurity program components identified within this book, you would have over 900 countermeasures defined within your defense-in-depth model. Sounds like a lot and it is. But remember, the devil is in the detail. In my opinion, not documenting your defense-in-depth approach is the number one reason why defense-in-depth fails many companies.

5.4 Open Source Software Protection

You may have already noticed that your IT organization has made the strategic shift toward adopting *open source software.* According to a recent market survey by Black Duck Software (Flomenberg, 2016), more than 78% of enterprises run on open source, and fewer than 3% indicate they don't rely on open software in any way. This shift to open source changes how security is applied within the defense-in-depth model. Not only do you need to be concerned about how to protect attack surface components that include open source software, but now many cybersecurity products are based on open source code. Ignoring the security of open source attack surface components can prove to be disastrous. A case in point is the September 2017 announcement by consumer reporting company Equifax, Inc. that a giant cybersecurity breach compromised the personal information of as many as 143 million Americans - almost half the country (O'Brien, 2017).

At the time of this writing, the full investigative report is incomplete; however, Sonatype Inc. the stewards of the Central Repository of the open source community published its analysis of the cyberattack, essentially laying the blame squarely at the feet of Equifax. According to Sonatype, "Organizations like Equifax are continuously deciding where and how to invest in cybersecurity based on a cost-benefit assessment, but at the end of the day they are ultimately liable for the security of their data and systems" (Weeks, 2017). Equifax, on the other hand, publicly blamed Apache's Struts open source software for its record-breaking security breach. The court of public opinion will ultimately decide if the open source community is responsible for building secure code or if organizations must accept the responsibility to secure the open source code they chose to deploy.

Many of my colleagues assert that open source software is inherently more secure because of the transparent nature of the way it is developed within an open community. They argue that many eyes are on the code to identify vulnerabilities and bugs. My position is that whether your organization uses commercial off-the-shelf (COTS) or open source software, you must follow proper cybersecurity practices. I have seen many companies lured into a false sense of security by thinking that either their COTS or open source software is more secure than it is. I recommend that you follow the advice in Table 5-9 - specifically the sub-domain of secure software development lifecycle component of software composition analysis - to begin planning for the security of your organization's open source software library. Virtually all aspects of this book can and should be applied to open source.

Here are my top tips for ensuring your open source library is secure:

1. **Adopt DevSecOps:** Ignoring basic blocking and tackling will cause you to lose the cyber war. Open source is introduced in applications development and your cybersecurity should be introduced at the same time.
2. **Identify open source code:** If you can't see it, you can't protect it. Commit to discovering all opensource through composition analysis.
3. **Monitor open source vulnerabilities:** If you let your guard down, you will get overrun. Acquire an alerting capability to provide notifications of new open source vulnerabilities.
4. **Patch vulnerable open source code:** Receive notifications from open source providers of new versions, releases, or patches. Rate each following your risk management approach.
5. **Monitor open source code library:** Continuously monitor open source code security performance, and conduct security training.
6. **Never assume open source code is secure:** Expecting someone else to do your security work is a failed strategy. Trust but verify all open source code.

If you're wondering why I haven't provided you with a *securing open source silver bullet*, the simple answer is that there isn't one. But if you follow the advice in this book and treat open source the same as any component of your attack surface, you just may avoid becoming the next Equifax.

5.5 Defense-in-Depth Checklist

To help you with the building of your defensive in depth strategy, I have provided a checklist in Table 5-14. This checklist pulls together the essential steps covered in this chapter in an order that will simplify all that you will need to do to achieve an effective defense-in-depth strategy.

Table 5-14. Defense-in-Depth Strategy Checklist

Step	Activity

1	**Finalize your attack surface – define the first dimension of your defense-in-depth model. Only select the layers that make sense for your organization. If your program excludes the supply chain, then exclude it from your model.**
2	**Adopt NIST CSF – use CSF as your second dimension of your defense-in-depth model. Align your existing cybersecurity countermeasures to each applicable NIST CSF category. Use table 5-4 as your legend.**
3	**Create a defense-in-depth schema –use an Excel spreadsheet using the template provided in Table 5-13.**
4	**Align countermeasures – align countermeasures to each category of the NIST CSF.**
5	**Document defense-in-depth – build a schema like Table 5-13 to document the defense-in-depth countermeasures.**

Summary

You now have a knowledge set that, frankly, many managers involved in their organization's cybersecurity program do not have. They have not had the benefit of over 30 years of building and maturing a cybersecurity program that you obtained by reading the first five chapters of this book. Think of yourself as having manufactured a fine European race car. But before you take it out on the track, you should learn how to drive it, right?

In the final chapter, I will show you how to operationalize the cybersecurity program that you have designed and built. Chapter 6 will cover everything from documenting your countermeasures in a service catalog to properly staffing the cybersecurity functions.

References

Chen, P. (1976, March). The entity-relationship model - Toward a unified view of data. *ACM Transactions on Database Systems*, 1(1), 10-36. Retrieved from http://www.comp.nus.edu.sg/~lingtw/papers/tods76.chen.pdf

Flomenberg, J, (2016, June 19). *The next wave in software is open adoption software.* [Blog post] Retrieved from https://techcrunch.com/2016/06/19/the-next-wave-in-software-is-open-adoption-software/

Gemalto. (2017). *2016 Mining for database gold.* Retrieved from http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf

Mitchell, B. (2017, June 9). Understanding the open systems interconnection model? *Lifewire.* Retrieved from https://www.lifewire.com/open-systems-interconnection-model-816290?_ga=2.101929281.1939442934.1495204556-1362401804.1495204

O'Brien, A. (2017, September 8). Giant Equifax data breach: 143 million people could be affected. *CNN Tech.* Retrieved from http://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html

Weeks, D. (2017, September 9). *Struts2 vulnerability cracks Equifax.* [Blog post]. Retrieved from http://blog. sonatype. com/ struts2-vulnerability-cracks-equifax

Chapter 6

Applying Service Management to Cybersecurity Programs

Even the best laid plans can come unwound if they are not executed properly. The same is true of your cybersecurity program. You can spend months if not years designing and building the prefect cybersecurity program, but if the program is not properly staffed and operated, your efforts will fall woefully short of expectations. This chapter shows you what is required to properly operate your cybersecurity program from assigning the right staff to implementing the right processes.

This chapter will help you to:

- Understand the importance of adopting a service management approach.
- Know how to implement security into your application development process.
- Identify the proper cybersecurity program roles and responsibilities.
- Learn how to automate and orchestrate cybersecurity program services.

6.1 Information Technology Service Management (ITSM)

Now that your cybersecurity program is designed, you will need to ensure that you operate it with the greatest effectiveness and efficiency. You will need to think of your program as a set of services delivered to protect your organization's assets and information. This is where *information technology service management* (ITSM) comes into play. ITSM is a term given to information technology (IT) activities driven by policies that are enforced by processes and supporting procedures to design, deliver, operate, and control services. IT activities are viewed as services rather than individual systems, applications, or products. Your cybersecurity program essentially becomes a service organization where an appropriate combination of people, processes, and technology combine to deliver a specific service to customers. Your customers are those you protect from cyberattacks. Service management provides several benefits:

- Alignment and focus on customers.
- Higher levels of service effectiveness and efficiency.
- Improved cybersecurity program reputation.
- Lower program cost.
- Predictable, repeatable service outcomes.

6.1.1 Brief History of ITSM and ITIL