In this package, you will find:

A Biography of the author of the book
A preview chapter from the book, Chapter NO.1 "Enterprise Security Overview"
A synopsis of the book’s content
Information on where to buy this book

About the Author

Aaron Woody is an expert in information security with over 15 years of experience across several industry verticals. His experience includes securing some of the largest enterprises in the world. Currently, he is a Security Consultant in the public sector. He is also a speaker and active instructor teaching hacking and forensics, and maintains a blog n00bpentesting.com.

Aaron can also be followed on twitter at @shai_saint. He will be launching a companion website (http://www.datacentricsec.com) for this book. To contact him for consulting please e-mail him at aaron.m.woody@gmail.com.

I sincerely thank my wife Melissa and my children, Alexis and Elisa, for sharing me with this project.

For More Information:
Enterprise Security: A Data-Centric Approach to Securing the Enterprise

Information security in the enterprise is challenging and has been considered a roadblock to enterprise innovation and use of new services such as cloud and bring your own device (BYOD). One of the primary reasons for this is the paradigm from which information security is being approached in today's ever evolving and agile businesses. Strict security requirements as an overlay to a perimeter-focused network architecture does not adequately secure enterprise data, failing the agile enterprise.

This book covers the current state of enterprise security and a new model for implementing security in the enterprise. Data-centric security architecture is introduced in the context of a layered security approach for end-to-end security. By looking at each component of the data-centric architecture, the realization of applying these concepts to information security creates a new paradigm to operate from where information security is agile and becomes a business enablement process supporting the latest trends in business such as cloud and BYOD.

The book is a guide to leveraging existing investment in traditional network- and host-based security tools. It introduces the data aspect of security and how to provide complete coverage of enterprise security. With several diagrams to illustrate concepts, and resources for further development in the areas of enterprise information security, this book serves as a go-to reference for IT professionals responsible for securing enterprise networks and data.

What This Book Covers

Chapter 1, Enterprise Security Overview, introduces readers to the concepts of information security by providing an overview of information security, where we went wrong, and the road map to securing the enterprise.

Chapter 2, Security Architectures, covers the drivers of redefining security architecture from a network-based concept to a data-centric focus as today's ever-changing business landscape has invalidated the traditional security architecture. The chapter introduces trust models and how they can be applied to existing data and infrastructure.

Chapter 3, Security As a Process, covers the importance of security as a process through policies, standards, risk analysis, and security review of changes. For security to be effective in the enterprise, it must be an integral component of everyday business processes.

For More Information:
Chapter 4, Securing the Network, is the first of several chapters diving into the layers of the data-centric security architecture. Methods to secure the enterprise at the network layer leveraging the latest technologies to mitigate threats at the network edge and segmented portions of the network are presented. The reader will also be given guidance on how to secure common network services.

Chapter 5, Securing Systems, presents methods to secure the systems that store, transmit, and process enterprise data. A look at effective approaches to securing systems when traditional methods fail is covered in detail. A list of tools is provided in Appendix C, Security Tools List.

Chapter 6, Securing Enterprise Data, presents readers with methods to secure data in the various states within the enterprise. Encryption, hashing, data loss prevention, and data classification are covered in detail to provide readers with several approaches to secure enterprise data.

Chapter 7, Wireless Network Security, provides coverage of securely implementing wireless networking in the enterprise. Methods to mitigate the most common and dangerous attacks against wireless are discussed. Lastly, the chapter covers proper segmentation of wireless infrastructure from critical segments and assets within the enterprise network.

Chapter 8, The Human Element of Security, takes a look at the weakest link in the enterprise security program: humans. The chapter examines social engineering and security awareness program development. Once a program is developed, consistent testing of the effectiveness of training is presented with several resources to get this portion of the program up and running.

Chapter 9, Security Monitoring, covers the many times overlooked, yet very important aspect of security monitoring. First, the chapter covers monitoring at the various layers of the new security architecture, then dives into leveraging SIEM solutions and providing monitoring for privileged users, systems, and the network.

Chapter 10, Managing Security Incidents, covers security incidents and management. Making the determination on what a security incident is and how to develop the response is the focus of this chapter. Guidelines for developing an incident response capability, along with supporting processes, are also provided to the reader.

For More Information:
Appendix A, Applying Trust Models to Develop a Security Architecture, walks the reader through applying the presented security architecture and trust models to a real-world scenario. This exercise will strengthen the new concepts presented in Chapter 2, Security Architectures.

Appendix B, Risk Analysis, Policy and Standard, and System Hardening Resources, provides a list of available resources to help the reader develop the necessary enterprise security processes: risk analysis, vulnerability and patch management, and policies and standards.

Appendix C, Security Tools List, covers a list of security tools that can be used to provide security at the network, system, and data layers of the data-centric architecture. In addition to tools for securing the enterprise, the reader is provided tools for testing security, vulnerability identification, and security monitoring. It also provides a list of available resources to help the reader develop the necessary enterprise security processes: risk analysis, vulnerability and patch management, and policies and standards.

Appendix D, Security Awareness Resources, provides the reader a jumping board for building a security awareness program in the enterprise. Resources to learn presentation and teaching skills are provided along with tools to facilitate social engineering testing. Lastly, the reader is provided links to security awareness training materials and safe computing resources.

Appendix E, Security Incident Response Resources, provides a sample incident response process flow along with sample incident response forms and resources for incident response.

For More Information:
Enterprise Security Overview

Today's enterprise security approach is the product of an elaborate façade created by for-profit security vendors and outdated perimeter-focused security architecture. The focus has been shifted from protecting assets to guarding the network edge, while data continues to be exfiltrated, and data breaches are at an all-time high. This shift in focus has created a cat-and-mouse game of securing the enterprise from the latest threats at the expense of our budgets, network infrastructure, creditability, and maybe sanity. In response, we have self-imposed several challenges in the security industry and created a roadblock perception for the enterprise security team and enterprise security program. Let's reset our focus on securing what is most critical to the enterprise, its data.

This chapter will cover:

- The complex façade of enterprise security
- The failure of perimeter-focused security
- An introduction to security architecture
- Challenges of implementing security in the enterprise
- A road map to securing the enterprise

The façade of enterprise security

In concept, securing the enterprise may seem like a binary statement or universally understood idea, but a common solution continues to elude us. We have been trained to think that if we take certain steps such as developing secure processes, providing security training, and implementing security technologies, then we have secured the enterprise. This is in fact the "façade" of today's enterprise security approach. Security is not binary in an enterprise and implementation should be approached with a flexible and agile security architecture based on risk to enterprise data, therefore making the implementation of security more gray than black and white.

For More Information:
The static and inflexible approach meets compromise when a solution does not fit into the defined security architecture introducing undesirable risk, followed by the fall of idealistic enterprise security. In order for us to get to where we need to be, we need to understand the façade of enterprise security and take a look at how we got to the idea of enterprise security that is driving security purchases and the security industry today.

The history and making of the façade

In the earliest enterprise networks, there was not much call for a DMZ due to there being no real Internet presence like today. One example of early networking that drew the attention of malicious users was enterprise dial-up networking connections. Modems were used to make outbound calls and accept inbound calls to primarily process batch jobs for large backend systems. Security of this implementation was not much of a concern because the phone numbers had to be known and the systems connected to the modems were expecting very specific data from the calling modem. Eventually, modems became the method used by network and system administrators to connect to the enterprise network remotely for support functions. This was an excellent out-of-band method to access critical network infrastructure. If security was enabled, there may have been DIP switch settings that enabled password security on the receiving modem. This was until war dialing became a method to identify modems in large banks of phone numbers for attackers to gain unauthorized access to the connected equipment or network.

War dialing is a method of dialing large pools of phone numbers looking for a modem attached to gain unauthorized access to a network. Non-local calling was expensive so this led to hackers exploiting Private Branch Exchanges (PBXs) using a method called phreaking. Phreaking is a method of sending tones through the phone to the PBX that tricks the PBX to allow the calls for free.

Specialized equipment was designed and sold to enterprises to provide security for the modem infrastructure. As more advanced networking technologies were developed and enterprise assets became accessible on the Internet, weaknesses in the systems and network security were quickly identified. Attackers were eager to exploit any vulnerability that was discovered. This behavior influenced network equipment manufacturers to begin developing security products to defeat specific security threats as they were identified. Point solutions were chosen not accepting that this was a "band-aid" approach that would fuel a narrowly-focused security industry.

For More Information:
As more threats were observed, more point solutions were developed to mitigate the threats. It was this natural progression of networking capabilities and threats that launched the security software and hardware manufacturing industry of today. We have continued this pattern of reaction-based development of security tools driven by mitigating specific threats as they are identified. In lockstep, we implemented the new technology to protect against the new "threat". Anti-virus, firewalls, intrusion detection/prevention, and other security technologies are the direct result of an existing threat, and are reactive.

Our efforts had been focused on securing the infrastructure and we forgot about the data, applications, processes, and users. It is easier to just buy the new technology of the day and support the illusion that we are secure from the "threat". This is the trend today. Advanced persistent threat mitigation became a hot topic because it became a real threat and instead of rethinking our security architecture, we purchased and implemented another technology, and probably implemented the solution at the network perimeter. This should seem familiar. We bought the story the security vendors had to sell. If there is a threat, buy our product and it will make you secure.

The next diagram shows the progression of point solutions being developed over time as new threats are detected. It also shows that detection and mitigation of threats becomes more complex over time as the threats themselves become more complex. As Threat 1 is identified, then Product 1 is developed to specifically mitigate Threat 1, and so on. We are seeing some traction in hardware and software that is capable of mitigating several threats. However, integration, management, solution scalability, and ability to provide deep coverage in all areas is yet to be seen. This continues the trend observed to date.

For More Information:
Having observed the history of enterprise security and the status quo reaction, we didn't realize we were buying into a false thought. So we implemented poorly-integrated security controls to address the enterprise's need to secure its assets while allowing business to continue. Unfortunately, what we designed was a relatively secure network perimeter instead of functioning, extensible, enterprise-wide security architecture. In fact, most developed security architecture is sound network design with an overlay of security that dictates what communication is allowed to and from the unique network zones.

Whether it is called a DMZ, a business partner zone, or a remote office zone, it is perimeter security by design and function. Until recently this made sense; though not true, it was thought that the known threat has always been external. Networks may have been large, but not overly complex, with multiple business partner connections or multiple DMZs. Typically, if there were services to be made available to an outside entity, we would place the assets providing the service in a perimeter zone, give it a name, and implement according to a defined security architecture. Such was the extent of implementing a secure solution.

This mentality has led to bloated security budgets, crowded perimeter zones, and very little increase in security. Because we have purchased and implemented the latest next-generation firewall technology, intrusion prevention systems, advanced persistent threat mitigation, data loss prevention, and file integrity monitoring, we think we have secured the enterprise. However, we have only increased the complexity in mitigating low-hanging fruit threats at the network perimeter and decreased our effectiveness in mitigating threats holistically. This is the security façade we've jointly created with our security software and hardware manufacturers.

Our current approach to security
We as a security industry have found ourselves in a unique position with significant changes in the way enterprises are conducting business. The late 1990s solidified the Internet as the premier method to market, provide services, and sell products in a global economy. This also meant that to be competitive, outsourcing of internal work would occur, remote access to critical systems was required, and more complex applications would be implemented with access to the most critical systems and data. This changed the threat landscape. Our focus became more on protecting all external threats, while losing focus on the most risky access we so quickly gave away, so that the business could grow.

For More Information:
Security architecture 101

In order to have a consistent approach to security, security architecture must be defined. Enterprise security architecture is the blueprint for securely implementing enterprise solutions to meet business requirements. Much like a house has blueprints for properly constructing it, security architecture serves the same purpose for the enterprise security design and implementation.

Up to this point, we have been discussing the implementation of security technologies as point solutions not necessarily as part of a defined security architecture. The progression of network technologies and business drivers created the first security architecture, but it was network focused and failed to address the enterprise as a whole taking into account data, processes, applications, roles, and users. Implementing to the network-based architecture with a security overlay limits the ability to sufficiently secure these components of the enterprise with agility and flexibility.

The current "security" architecture addresses user access to data in a very generic manner, focusing primarily on what protocols can be used at what tier of the network regardless of who the user is, the application used, type of data, and data interaction. An example of this approach is shown in the following diagram:

```
<table>
<thead>
<tr>
<th>Network Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
</tr>
<tr>
<td>Application</td>
</tr>
<tr>
<td>Data</td>
</tr>
<tr>
<td>User</td>
</tr>
</tbody>
</table>
```

If the approach for securing the enterprise is to constrain all solutions the enterprise implements into this defined "security" architecture, then there will be three possible outcomes:

- Implementation in accordance with defined security architecture; there is no deviation from design or defined security architecture
- Implementation in accordance with security architecture cripples the solution and implementation of the solution is aborted
- Implementation not in accordance with security architecture weakens the effectiveness of the security architecture to make the implementation successful and introduces risk to the organization

For More Information:
This inflexible security architecture often requires the enterprise to quickly decide if the "risk" of not following security architecture is acceptable or if another method is available to secure the implementation without jeopardizing the project (investment on the table). By risk, I am presenting the fact that this is usually a determination of whether properly securing the implementation is too costly and difficult versus accepting the perceived risk and proceeding with the implementation. To reduce the risk associated with not following the architecture, compensating security mechanisms may be implemented. A continued cycle of this resolution leads to an overall less secure enterprise.

Let's look at an example of our current method of implementing security in line with our common and generic security architecture. Today, we have done a good job at creating segmented networks at least at the network layer using virtual LANs (VLANs), internal firewall segmentation slowly being introduced, and assigning our users to groups according to job functions. I am careful to imply we have commonly defined roles within our architecture, so I will use functions, usually no more than a team designation. An example would be a VLAN called DBA_VLAN that is for the database administrator job function. Each VLAN will have its own unique IP subnet, so the database administrator "team" can easily be identified by the IP address of their system on the network. We can then implement firewall rules (if implemented) to allow this unique IP subnet access to the systems with databases. This is a very simple implementation and very ineffective security. In this previous example, the only unique identifier is the IP address in an assigned IP subnet belonging to the database administrators. This method does not constitute a secure authentication method, which should be more granular and performed at the user level.

The teams responsible for the security of the databases would present that the database security itself is the most important, so it doesn't matter who is sitting on the DBA_VLAN because ultimately only authenticated individuals can access the database systems. Unfortunately, this architecture allows for many misuse scenarios that increase the risk of a data breach through unauthorized access over trusted communications. We may have implemented security mechanisms, but I am willing to bet they are threat specific and lack the broader threat perspective required to secure the implementation. This is not security architecture, it is security patchwork often focused only on the product side of security because we have never figured out how to properly secure our people through roles, processes, policies, and standards. The example presented is the unacceptable yet accepted norm; recent data breaches have proven this is not a sufficient method to secure data.
A new approach to security

Our approach to securing the enterprise should go beyond simple threat mitigation. After all, this is exactly why we are in the not-so-effective security state that causes the breaches we see regularly in the news. As with all good design and architecture there are many factors that must be taken into consideration to properly influence the correct implementation. There is network infrastructure, system architecture, applications, and data that need to be designed, implemented, and secured. There are also people and systems that will access these components provided by the enterprise to use a service, and so on.

I recently traveled to Savannah, Georgia (GA) and was able to appreciate this very principle in home and building architecture and design. Did you know that any home built in historic Savannah has to be externally period correct? The requirement is to maintain the well-thought-out and aesthetically pleasing architecture. The original architects had many influences and deep reasons for the materials, layout, functionality, and design of the buildings at different points in history. Each home and building was not approached with a single thought or idea for its only purpose; instead, there is a standard that must be followed. The architectural standard allows the construction of new homes with modern amenities inside, but the exterior must fit it to the surroundings. Owners of the homes can decorate the interior how they please; this is the uniqueness of each home allowing each home owner to have the home they want without introducing architectural anomalies to Savannah. As architects design and plan a new home build in Savannah, GA, we should approach security architecture with the same broad, yet focused vision in the enterprise.

With the previous database system access scenario fresh in our minds, what would be more of an architectural approach? First, should security architecture rigidly define how this access should be granted, or can a more flexible approach be leveraged? I think the best first step would be to back up and take a broader look at the requested access. If we can understand the criticality of the data/system based on the data or function, what type of access is needed, why the access is needed, who or what will access the data/system, then we can determine the risk and better develop an architecture that properly secures the data/system and provides the access needed to allow the business to function. The issue we most often run into is we jump right into figuring out how we are going to secure something, whether it is networks' communications, system access, or whatever, without any idea what (if any) risk is introduced. The other issue is, since we have focused so much on securing the DMZ, we haven't properly architected security further into the infrastructure, at least not more that the typical firewall, IDS/IPS, and maybe some system security products, so we are forced to either make expensive purchases or compromise on security.

For More Information:  
Unless we develop a new security architecture—an architecture that addresses all facets of security and provides a realistic picture of the risk posed by any implementation—the secure enterprise will never be realized. The new approach to security architecture takes into account data, processes, applications, user roles, and users, in addition to the traditional network security mechanisms to provide end-to-end security from entry to the network to the data resident within the enterprise. The following diagram shows a more comprehensive approach to security based on risk of the entire interaction with enterprise data:

![Diagram showing a more comprehensive approach to security based on risk of the entire interaction with enterprise data.](image)

**Enterprise security pitfalls**

The challenging responsibility of leading security within an enterprise can be successful or disastrous. Security in principle is black and white, however, implementation and the real world is gray. When security personnel operate from a binary perspective on security principles it fosters a false perspective of an ideal enterprise security posture. It does not exist and will frustrate security objectives. We as security personnel are charged with understanding how the enterprise functions so that we can provide the desired security direction and expertise as a business enabler. We can then more effectively determine risk associated with implementation, and risk identification will determine investment is securing the implementation.

Many times the security conversation is nothing more than just that, a conversation, because the security team is unable to speak in a language the business or other IT teams can understand, let alone in a compelling manner to influence change if a solution will introduce risk or undermine security. If we are insisting that certain technologies must be implemented, then we must be able to bring this full circle and tie this position to supporting processes, policies, standards, business needs, and risk.

For More Information:
Application developers are a great example of a team that typically steers clear of point solutions and looks for options that easily insert into their existing processes and are repeatable. Working closely with other IT teams will prove to be fruitful and help achieve security-focused goals when collaboration and cooperation are encouraged to collectively decide on security solutions.

**Shortcomings of the current security architecture**

The current security architecture is not meeting the current enterprise trends such as **bring your own device (BYOD)** and cloud initiatives; it also does not address the internal network facet of information security. This gooey, soft inside has traditionally been neglected because the current security architecture deemed internal assets, employees, contractors, and business partners as trusted. The same security controls are typically not mandatory for the internal communications as in the perimeter, however, this is where an enterprise’s most sensitive and critical systems and data typically exist.

Example shortcomings of the current security architecture are:

- It fails to secure internal assets from internal threats
- It remains static and inflexible; small deviations circumvent and undermine intended security
- All internal users are equal, no matter what device is used or if the user is a non-employee
- Security is weak for enterprise data; access is not effectively controlled at the user level

We have done what the security industry vendors want us to do, buy security appliances and software and implement them, regardless of whether it actually increases the security posture of the organization. Some trends indicating we are doing it wrong are the significant increases in data breaches and more moves of security implementation to the cloud and other managed security services. This is indicative of implementing point solutions with little to no integration, limited in-house expertise and/or staff, and the overwhelming amount of data produced by the solutions. So while we have done all the correct surface things, we have in fact produced little positive impact, while complicating security.
What do we do when an implementation cannot be implemented per this current "security" architecture, or access that is requested causes the architecture to be broken? We compromise; not only on the architecture, but on the security of the enterprise. New security architecture must be developed to address the issues outlined. The remainder of this book presents a methodical approach to better positioning security in the enterprise and looks at how to implement flexible and agile security architecture to enable the business to take advantage of the latest trends.

Communicating information security

The zealous security professional will often focus so intently on the responsibility of securing the enterprise that they miss the business objective. This leads to security personnel having tunnel vision and only seeing one set of methods to secure an enterprise. This tunnel vision can be detrimental to the success of the security team overall and can have a negative influence on design and purchasing decisions.

Because security is not a commonly and generally understood IT function, it can be difficult to get upper management and other IT teams to give buy-in. This is evident when security is asking them to make costly network changes, or change the way a solution is to be implemented and the security team has failed to provide a compelling rationalization to do so. Why is this? I think, because we have not spent the time to understand how the business functions and we do not always have representation at the highest levels to present our case. In my experience, organizations that are missing a security focused executive-level sponsor are at a significant disadvantage of successfully implementing a security practice that really reduces the risk to business. What an individual at this level can achieve far exceeds the capability of management at a lower level because of the position of influence. It is much easier to influence laterally and downward, but very difficult to influence upward.

Discussions at lower levels within an organization tend to be more shortsighted, specific to an implementation, and more emotional. For example, when security becomes a topic during an initiative, the implementation of this initiative may be an individual's or team's vision, and now security is seen as threatening to complicate the implementation or halt it, maybe at an additional expense. Often, security is an afterthought, and is therefore not well received. Having a security-focused senior management position or having a security architect (team if needed) that is responsible for the overall security architecture of an organization can avoid or lessen the burden of this scenario. It should be noted that all enterprise employees are responsible for security and must embrace the integration of security into all applicable IT and business processes. The security of the enterprise is only as good as the weakest link.
The cost of information security

If security is communicated as an enterprise priority and is generally understood, we might think that we should be able to do whatever it takes to secure the enterprise. However, this is not necessarily always the case. At some point the cost valuation has to be determined before an enterprise makes a decision to take on additional expense to implement security controls. The difficulty in providing quantifiable data to back up the cost and request for security-related purchases is significant; we must learn to operate smarter according to more intelligent security architecture.

Let's think of it like this. If an intangible is presented such as if we buy security product "X" we reduce our risk of being hacked costing the enterprise a high-dollar figure and another team is presenting an expense that is tangible and quantifiable, where do you think the money will go? An example is: the security team wants to spend $150,000 on a web application firewall; there is no data on current attacks against the enterprise, just the latest report on the Internet showing the trends in data breaches associated with web application security. Another IT team needs to buy servers because the current servers are at capacity and without the purchase, several key IT initiatives will be impacted. This is not to say the latter is not valid, but this budget contention will always exist with the server team or some other IT team. Again, I ask, where do you think the money will go?

It is rather predictable because security has become a bit of a cat-and-mouse game, and we are losing. So the next best thing to winning is detecting and mitigating last year's threat. This makes the security budget every year a bloated figure that leaves the security team vulnerable to not being able to properly secure the enterprise and fighting for every cent to do so.

The overall reason why this is the case is due to the failing security architecture of yesteryear that we keep trying to shoehorn everything into. There are methods to reduce the security spend by making more intelligent business-focused decisions, that allow the business to be agile without compromising security, or at least with reduced risk.

The conflicting message of enterprise security

We as a security industry are too focused on one thing, "numero uno". That is to say that no one apparently in information security seems to be interested in actually solving the issues we face, but just to profit by keeping the well-oiled machine running. We have factions within security that say "do this, don't do that", while other groups are saying the opposite. This leads to teams of security personnel having very different ideas and views on how to implement security for the enterprise, determine risk, and handle day-to-day security operations.

For More Information:

An example of this conflicting message is the great debate on the subject of penetration testing and the false sense of security some believe it produces. There is great benefit to be had by consistent testing of enterprise security. The issues as observed are the lack of business justification, "value-added" when there is a lack of quantifiable findings, and knee-jerk reactions of buying something that probably won't fix the real problem identified.

Our trusted security vendors generally develop other conflicting messages on what the real issues are and how only their product or service is the solution. Remember, each has the best solution for you, choose wisely. One will recommend their file integrity monitoring, another their whitelisting application, and yet another will recommend their next-generation firewall. What is management to do? The best solution will have to be determined once the proper security architecture has been developed and accepted at the highest levels of the enterprise. Execute to this, not the latest marketing slicks.

Enterprise security is truly a risk-centered balancing act between business initiatives and security. The vendors will sell their products and experts will have their opinions. However, ultimately the enterprise security professional will need to decipher how each impacts the security posture of their respective enterprise. Once this logic is applied, the message is no longer conflicting because you, the professional, have made sense of the messages for your application of security. It may be difficult to get other IT teams to see the same perspective. Communicating security tool effectiveness and the expected impact to risk reduction and securing the enterprise will be the best way to decipher the sometimes-confusing messages communicated by the security industry.

Proving a negative

One of the most significant challenges in information security is proving a negative. This is to say for example, if specific steps, or actions are taken or a specific technology purchased, we are preventing what would be successful network intrusions. This is in part because there is no technology deployed that will give us this information and in part because we only learn of a small portion of breaches. Even if breaches are reported they may not happen in the same industry vertical or may lack pertinent details, and therefore do not provide any meaningful statistical data to justify security expense.

For More Information:
It is a challenge to get the executive board or other IT management excited about information security, and the price tags of the line items on the annual security budget. The traditional approach to information security decision making will fall flat on its face without a well-defined security architecture that is understood and adopted by those who will ultimately approve information security spend. This will have to be carefully approached using any and all applicable data that can support the position of the security team.

Ultimately, you can never prove the negative or convince senior management that changes need to be made in order to properly secure the enterprise without compelling data. A feasible method may be a well-written business presentation of applicable threats, assessed risk, and a recommended mitigation strategy for the enterprise. Also, providing a road map can be very useful if significant cost is associated with getting the enterprise to a proper security posture. Realizing this is an ever-evolving and moving target, a roadmap can allow for flexibility in strategy implementation over a period of time.

The road map to securing the enterprise
The road to a risk aware secure enterprise does exist; it is challenging, but tangible. In this section, I will lay out a road map to developing flexible security architecture as the foundation to securing the enterprise. It is not the only method, but it is sound and will hopefully serve as an exercise to challenge enterprise security teams to rethink the current architecture and security methods being implemented.

Road map components
There are several exercises that must be completed to obtain an accurate representation and definition of the enterprise assets (systems, data, and so on), communication methods, users, roles, business processes, policies, and standards. Each will need to be defined in extreme detail to be most effective, but if this is the first attempt a more generic definition of each can be the starting point, with a gradual increase in detail, until everything is defined and all possible combinations identified. The road map provided is an introduction to the detailed approach in the next chapter.
Starting with user groups may be the easiest, however, you can focus on systems and data in the beginning phases, especially if there has been absolutely no data classification or critical system identification. All of this data will serve as input to the trust models we will develop in the next chapter. Here we will provide an overview of what should be collected for each defined component. It should be noted that all components need periodic review, and recertification should be built into the process. A simple diagram of the process at a high level is provided as follows:

**Defining users**

All users within the enterprise and those that interact with the enterprise, such as contractors and business partners, must be identified and their relationship with the enterprise determined. This data will provide input to roles and start tying the relationship of an individual or group of individuals to data.

**Defining applications**

Define all applications in the enterprise, their purpose, and what data they are used to access. It is also important to understand what systems the applications are installed on to determine scope when identifying risks associated with application access.
Defining data
This may seem very simple, but it can prove to be a difficult task even for the smallest enterprise. Each department may have different data, and subjectively valued, it may not be defined in the perspective of overall value to the enterprise. Additionally, identifying where the data resides, such as which systems or physical locations, is a key issue. Things to consider are duplication and backups of the data. Data may reside in desktop applications such as Microsoft Access with databases duplicated many times over for each user that needs access residing on the user systems. Additionally, data should have a classification assigned per policy that dictates the required security for the identified data and may need to be in compliance to HIPPA, SOX, PCI, and other regulatory requirements. Data is the focus, as typically systems have no value aside from the expense of the physical hardware and the data that is contained within them.

Defining roles
Once users and data sets have been identified, the purpose of the access must be defined. For instance, basic user access versus administrator access. There are also data custodians; perhaps our trust model will have additional monitoring requirements based on the level of access to critical data. These roles can start as generic, but the more defined the user group and roles are, the better the user interaction will be understood and the more granular the controls that can be implemented.

Defining processes
Defining business processes will often lead to identification of the business critical data and systems. Understanding the processes that make the enterprise function can also identify additional users and roles not previously identified. Examples of processes are automation, change management, and third-party oversight.

Defining policies and standards
Once all users, roles, and processes have been defined, there must be some policy that dictates what is permitted use of the authorized access, and defines what is unauthorized behavior while using the enterprise assets including but not limited to: network, applications, systems, and data. Standards by which users are to be provisioned, access to applications, data, and systems to be handled should be standardized to ensure consistency. Standards will also include items such as system builds and security, security configuration of applications, and security monitoring.

For More Information:
It is important that the enterprise is willing to take action if there is a violation of policies and standards because it is implied that deviation from these will introduce risk to the enterprise and possibly undermine security, resulting in a data breach or other negative impact to the enterprise.

Defining network infrastructure
This process requires understanding what has already been implemented to facilitate business partner communications, external access via website, VPN access, and so on. Having defined the network "zones" and the users, both internal and external, that use them will drive the required security monitoring and protection mechanisms. In some cases once this exercise has been completed, it may be determined that a new zone needs to be created and implemented to support the security initiative of the organizations.

A layered approach to security that includes network infrastructure is critical to an end-to-end secure enterprise. Ultimately, the preceding component definition should drive much of the network architecture, where applicable, requiring the network and security teams to work closely in these areas of the infrastructure. There must be consistent standards, especially for the network infrastructure, as it provides all the connectivity for business network communications.

Defining application security architecture
Applications are the preferred method for accessing enterprise data. Understanding how security is integrated into applications through a formal Software Development Life Cycle (SDLC) will not only provide useful data for trust models, but may also highlight other areas that need additional security implemented to meet the standard of the application. Standards for data protection can be gleaned from the secure development processes that can be used in other areas of IT.

Summary
We as security professionals have become used to the idea that security is a state to reach, but it is unattainable. In part, because the old security architecture no longer meets the enterprise needs, and because we have not adopted a more intelligent architecture that is focused on enterprise data and risk. There are several challenges that the enterprise security teams must navigate. This chapter introduced concepts that will be further explored in this book and that will address these challenges and provide a methodical approach to securing the enterprise with the adoption of a new, flexible, and agile security architecture.
Where to buy this book


Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our shipping policy.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.