Your Most Comprehensive Cybersecurity Plan

BUILT LAYER-BY-LAYER

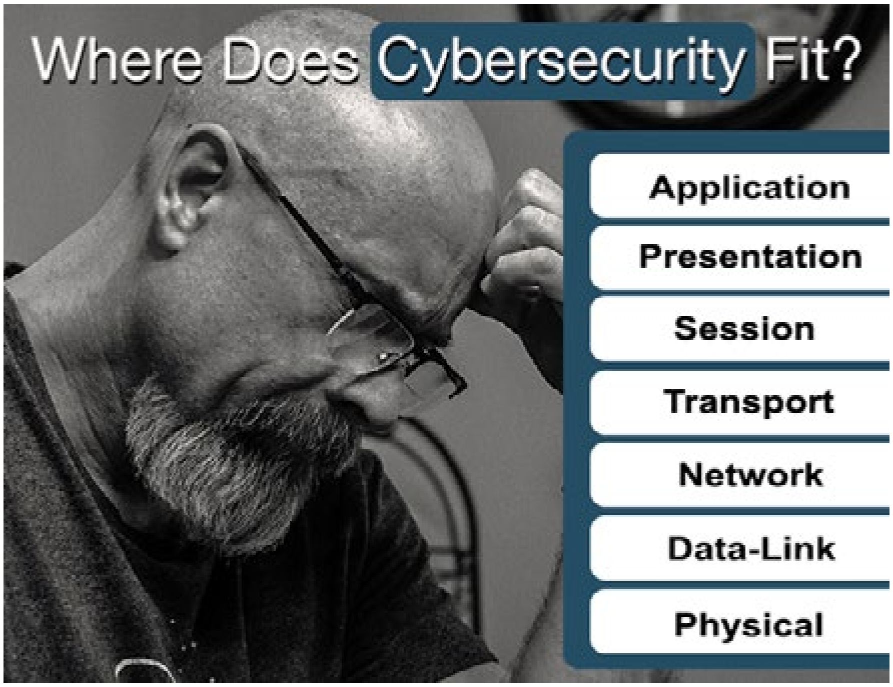
New Horizons®
Computer Learning Centers

Comprehensive. If there's one most important yardstick for determining the effectiveness of a cybersecurity plan, it's the measurement of how comprehensive it is. Always think of cybersecurity as being the chain that is only as good as its weakest link. Your plan must address every link in a comprehensive cybersecurity strategy.

The Missing Security Layer

Technology professionals think of networks as being structured in seven levels or layers. We can think of these layers as the "links" in our metaphorical chain. A little background on this:

In 1983, the International Standards Organization (ISO) introduced a useful seven-layered model for networked computing called the Open Systems Interconnection (OSI) model.



Here is the reality; if security is not efficiently embedded into every layer of the ISO-OSI model it is vulnerable and ineffective

Moving outward from the user, data is entered into the network through software running on the Application layer. This application is running on a device-based operating system at the Presentation layer which is signed in through the Session layer. Data is moved from that user to another destination by the Transport layer which uses the Network layer to connect to that destination. This connects to the actual network via a network interface card at the Data-Link layer which, finally, connects to the actual cabling and wireless infrastructure at the Physical layer.

Arriving at the other end, the data travels back up the seven layers to arrive at its intended destination. Each layer has its own protocols and other communication standards that govern its efficient operation.

So, you may be asking, where is the Security layer? Where does security fit in?

The answer is “Yes.”

Unless every layer of the network is secured, penetration can occur. Data can be compromised.

Imagine a building with seven doors providing entry. If all seven doors are locked, the building can be considered secure. If one is left unlocked, the entire building is insecure. It really is just that simple. Unless every layer of the network is secured, penetration can occur. Data can be compromised. And compromised data creates an existential danger. According to Inc. Magazine, 60% of businesses whose data is significantly compromised go out of business and don't return.

Many providers of data and network security products emphasize the importance of "multi-layer" security, but here is the reality; if security is not efficiently and effectively embedded into every layer of the ISO-OSI model, every step along the path data takes from origin to destination, it is vulnerable and ineffective. Only as secure as its weakest link.

Security Threats at Every Layer

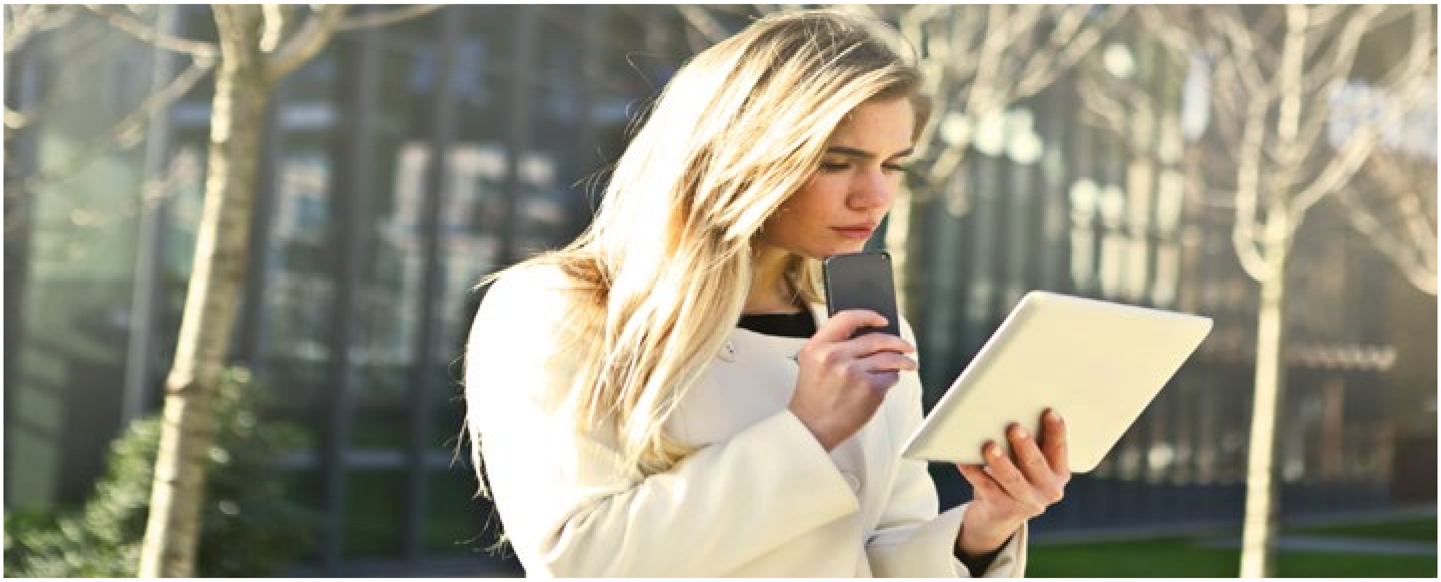
If security must exist at all layers it's because there are threats to each layer. We start at Layer 7 – the Application Layer because that's where every transaction begins. As mentioned earlier the data travels down the stack of layers, across the physical layer cable or wireless connections, and back up the stack on the other side. The place where users begin by interfacing to the network is at the application, layer 7.

Users are human and far more subject to making costly errors than are computers and other digital devices which will perform the same function the same way every time.

For the purposes of creating our cybersecurity plan we must actually start BEFORE the Application Layer and address perhaps the biggest vulnerability in the entire network – the user. Users are human and far more subject to making costly errors than are computers and other digital devices which will perform the same function the same way every time.

The best example is what is currently the most prevalent threat in the cyber landscape – ransomware. Fraudsters send out a "phishing" email that looks very authentic, very much as if it actually comes from where it says it does. But somewhere in that email is a link for the user to click or an attachment for the user to open. The text provides powerful inducements to get the user to do so. Once they do their data is either encrypted, corrupted, or stolen. The only way to get it back is to pay a ransom, thus ransomware.

The attackers know the user is their best place to gain access.



Threats at each layer of the ISO-OSI model include:

1 Application Layer Threats

Security software developer F5 tells us, “Examples of application layer attacks include distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and Slowloris attacks. To combat these and more, most organizations have an arsenal of application layer security protections, such as web application firewalls (WAFs), secure web gateway services, and others.” The team at SecurityIntelligence points out that, “The application layer is the hardest to defend. The vulnerabilities encountered here often rely on complex user input scenarios that are hard to define with an intrusion detection signature. This layer is also the most accessible and the most exposed to the outside world. For the application to function, it must be accessible over Port 80 (HTTP) or Port 443 (HTTPS).” Other possible exploits at the Application Layer include viruses, worms, phishing, key loggers, backdoors, program logic flaws, bugs, and trojan horses.

In the regular maintenance portion of your plan be sure to remind operators to check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability.

Your cybersecurity plan must include Application Monitoring which is the practice of monitoring software applications using a dedicated set of algorithms, technologies, and approaches to detect zero day and application layer (Layer 7 attacks). Once identified these attacks can be stopped and traced back to a specific source.

2 Presentation Layer Threats

The most prevalent threats at this layer are malformed SSL requests. Knowing that inspecting SSL encryption packets is resource intensive, attackers use SSL to tunnel HTTP attacks to target the server.

Include in your mitigation plans options like offloading the SSL from the origin infrastructure and inspecting the application traffic for signs of attacks traffic or violations of policy at an applications delivery platform (ADP). A good ADP will also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure.

The most effective protection is achieved by consistently observing best practices for router, firewall and switch configurations.

3 Session Layer Threats

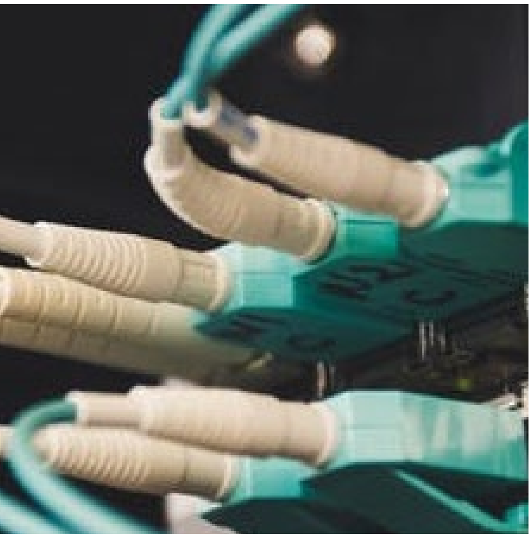
DDoS-attackers exploit a flaw in a Telnet server running on the switch, rendering Telnet services unavailable.

In the regular maintenance portion of your plan be sure to remind operators to check with your hardware provider to determine if there's a version update or patch to mitigate the vulnerability.

4 Transport Layer Threats

According to Network World, "Many businesses use Transport Layer Security (TLS) to secure all communications between their Web servers and browsers regardless of whether sensitive data is being transmitted. TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is an IETF standard intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail and voice over IP."

5 Network Layer Threats



Routers make decisions based on layer 3 information, so the most common network layer threats are generally router-related, including information gathering, sniffing, spoofing, and distributed denial of service (DDoS) attacks in which multiple hosts are enlisted to bombard a target router with requests to the point where it gets overloaded and cannot accept genuine requests.

The most effective protection is achieved by consistently observing best practices for router, firewall and switch configurations. At the router itself it is important to constantly assure that the router operating system is up to date on all security patches, packet filtering is kept enabled and any unused ports are blocked, unused services, and interfaces are disabled. Keep logging enabled and conduct regular auditing of any unusual activity that may occur.

It's also advisable to place firewalls between your network and all untrusted networks. Always keep that firewall up to date with all issued security patches, enable packet filtering, and keep logging enabled so you can audit any anomalies.

Any switches on your network must also be kept updated with all security patches, with any unused interfaces or services disabled. Make certain that all switch traffic is encrypted.

6 Data-Link Layer Threats

Cisco explains that, “The data link layer provides reliable transit of data across a physical link. The data link layer is concerned with physical, as opposed to logical addressing, network topology, network access, error notification, ordered delivery of frames, and flow control. Frame-level exploits and vulnerabilities include sniffing, spoofing, broadcast storms, and insecure or absent virtual LANs (VLANs, or lack of VLANs). Network interface cards (NICs) that are misconfigured or malfunctioning can cause serious problems on a network segment or the entire network.”

“The data link layer provides reliable transit of data across a physical link.”

Most companies that have experienced Address Resolution Protocol (ARP) spoofing, Media Access Control (MAC) flooding or cloning, Port Stealing, Dynamic Host Configuration Protocol (DHCP) Attacks, layer 2-based broadcasting or Denial of Service Attacks have immediately focused on improving port security. They also configure their switches to limit the ports that can respond to DHCP requests, implement static ARP and install Intrusion Detection Systems (IDS).

7 Physical Layer Threats

Ask any networking professional to define where the network is and they'll point at "the wires in the walls." What they're saying is that the copper and fiber-optic cables that connect everything together create the actual network that everything else uses. Most threats at this layer involve interruption of the electrical signals that travel between network nodes including the physical cutting of cables, natural disasters that bring flood waters which can cause short-circuits, or other human vandalism.

Many companies mitigate these failures by bringing in multiple circuits to the internet. It should be noted that this works well until a backhoe digs up a critical corner through which all carrier circuits run, thus disabling all of the multiple paths. The aftermath of many disasters illustrates the superior strategy being the placement of all network core elements such as servers and storage at multiple redundant cloud data centers. Should a major carrier cable be cut, only users will be affected, and they can switch to wireless access or other locations until repairs are completed.

The Best Offense is a Great Defense

Just as true in cybersecurity as it is in athletics, building and maintaining great defense lifts an operation out of constant “fire-fighting” mode and up to a place where it can be proactive about growing the business.

The thing to remember is that great cybersecurity begins with great security planning. As Benjamin Franklin advised, “A failure to plan is a plan to fail.”

Since users are our most unpredictable network component it is critical that your plan address best practices and operating requirements on your network, but the plan is equally important to the digital devices that help create the comprehensive defense we’ve been discussing. The purpose of a firewall, for example, is to enforce your security policies and rules. That’s not possible if you have no security policies and rules.

In the case of cybersecurity, a failure to plan is a short-term strategy. Attacks will happen, and they will disrupt and disable operations, which is ultimately an existential hazard.

A failure to plan is a plan to fail

Internet of Things and Mobile

According to research presented in a Cisco infographic, the number of “things” connected to the internet exceeded the number of people connected way back in 2008, and many analysts started reporting that there were more mobile devices on Earth than people starting back in 2014. Every one of these billions of things and mobile devices must be secured.

Picture every mobile device as a door into your network. Using bare minimal security that comes pre-installed on the device renders it a flimsy door.

Effective security is achieved by observing best practices, including:

“Always On” means Always Vulnerable – Every mobile device has multiple ways of communicating with other devices, including wi-fi, 4G-LTE, and Bluetooth. While it may seem more convenient to leave these switched on at all times, that is the equivalent of leaving doors open at all times. When not in use, switch them off.

Keep Up with Updates – While some updates may be time-consuming, it is important to implement them especially when they are security updates. These were probably created in response to attacks that already happened and can still happen to those unprotected by the update.

Effective security is achieved by observing best practices, including:

Use Strong Passwords and Multi-Factor Authentication Where Available – Many mobile services enable multi-factor authentication in which they will send a code upon login attempt. That code must be entered following the password. Passwords should always contain letters, numbers, capital letters, and special characters to keep them almost impossible to "figure out."

Brickable – Effective mobile management systems include the ability to "brick" a lost mobile device, removing all data and software completely via remote signal. The data is far more valuable than the device itself.

The Value of Skepticism – There are plenty of attractive looking apps out there, but the installation of one that contains malware can be disastrous. Approach each application with deep skepticism. Prove to yourself that its from a valid developer and is safe.

Default to Defense – Many applications and operating systems are installed with many security settings switched off. Wherever and whenever possible switch these on. While it may be less convenient operating your device with more security measures activated, nothing is less convenient than having to recover from a successful attack.

A hacker reaches into the building's ICS and shuts down all air conditioning.

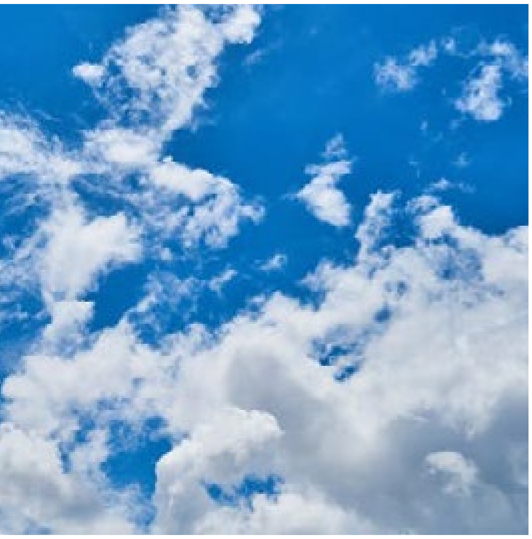
To fully appreciate the exposure created by Internet of Things technologies, consider how Industrial Control Systems (ICS) work. Sensors are deployed throughout a building that measure ambient temperature, lighting, and presence of people. These all report back to the ICS which adjusts thermostats, opens and closes vents, and turns lights on and off based on current conditions. If nobody is present in a section of the building, services to that section may be turned off. Not only does this assure comfort and convenience, it also dramatically reduces expense for power consumption and HVAC.

Now imagine a building in Phoenix, Arizona or Houston, Texas in the middle of summer. A hacker reaches into the building's ICS and shuts down all air conditioning. Talk about disruption of operations, it isn't long before everyone working in that building must stream out to escape the stifling heat.

Exploited cameras may provide unauthorized parties visibility into offices and other locales. Exploited microphones in internet-attached devices such as personal assistants, once compromised, become an invisible eavesdropper.

More broadly, every "thing" connected to a network provides access challenges similar to mobile devices. Each one can be compromised, turning the billions of "things" into billions of potentially open doors to networks. It is critical to plan security into every "thing" that will be installed.

SECURING *NEW* TECHNOLOGIES



The Cloud

There is a popular misconception that security in the Cloud is supplied by the cloud service provider.

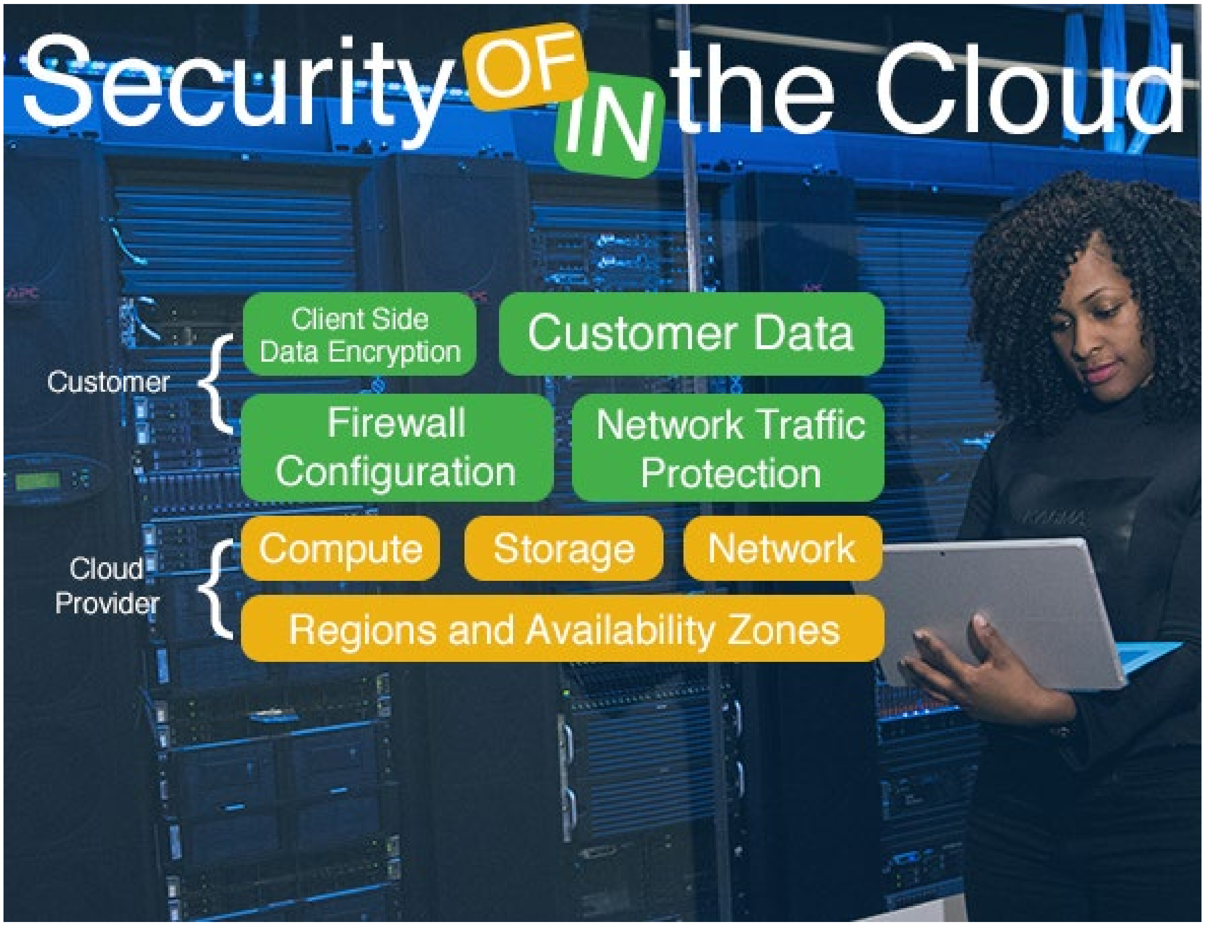
While security provisions may be furnished, fiduciary and legal responsibility for the safety, security, and privacy of data remains with the cloud customer. Beyond criminals you are exposed to governments. Many cloud providers will immediately comply with any subpoena they may be served with, and they are not required to notify you when your data was the subject of a subpoena.

Beyond complying with all security provisions furnished by the cloud provider, including advanced authentication and authorization processes, it is critical that every company encrypt all data in transit and at rest in cloud storage.

It is critical that every company encrypt all data in transit and at rest in cloud storage

Encrypted data is useless to any criminal who may manage to get past the cloud provider's protection, and data surrendered under subpoena is useless to governments who don't have the decryption key. Since they must come to you to demand the key, you will become aware that they have obtained your encrypted data and can take any legal action you deem appropriate.

One of the key advantages of cloud computing is realized when you advance to multi-cloud environments. Remember that each cloud provider has their own security protocols and standards and you must prove to yourself that all participants in your multi-cloud solution integrate seamlessly with each other.



Containers and Microservices

Traditional software development produced large, all-inclusive applications. Today these are referred to as “monolithic” applications and their biggest challenge is that if something goes wrong it may bring the entire application down causing operational disruption until modifications can be achieved. Another challenge is that it is often difficult for new programmers to improve upon or even understand what their predecessors had done in writing the original code.

More recently, developers of code and operators of the systems that run it realized that more could be accomplished by aligning their operations, tools, and practices. This has resulted in the creation of DevOps.

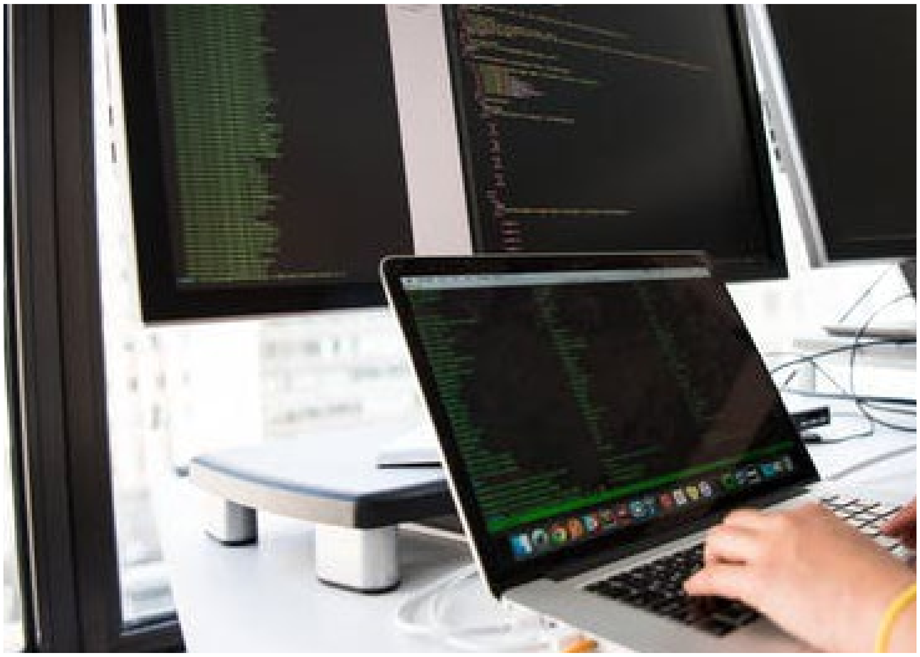
One of the primary goals of DevOps is to achieve continuous improvement through continuous development and deployment (CI/CD). This calls for rapid release of new code improvements followed by immediate feedback gathering by the operators who feedback to the developers who create more new improvements and repeats the cycle as the operators deploy the new code.

It is often difficult for new programmers to improve upon or even understand what their predecessors had done in writing the original code

The key to DevOps success lies in keeping everything moving quickly. Development, Deployment, Feedback, Repeat. Monolithic programming doesn't lend itself to rapid improvement.

Microservices do. In this exploding development environment applications are created as an assembly of many microservices each of which performs a specific function. As that function is needed, an instance of the corresponding microservice is released in a container that includes all of the libraries and other resources required for that microservice to function. This modularity and completeness of packaging lends itself perfectly to the distributed processing nature of cloud computing.

There are multiple points of vulnerability which must be addressed to assure the security of containers and their microservice payloads.



There are multiple points of vulnerability which must be addressed to assure the security of containers and their microservice payloads.

Secure the Container Host

Select a reliable, well-supported container-focused operating system to host your containers. This will help reduce your overall attack surface by removing services that aren't required to host your container workloads. Add monitoring tools so you are aware of the health of the hosts. Using a managed container service from a reputable cloud service provider eliminates the need for you to manage this. They secure the host on your behalf and you simply run your containers.

Secure the Networking Environment

Traffic moving to and from the internet should leverage an Intrusion Prevention System (IPS) and web filtering in order to stop attacks and filter malicious content. An IPS should also be deployed to monitor traffic between containers.

Secure the Management Stack

Ensure that your container registry is properly secured and monitored. Lock down your Kubernetes installation and take advantage of features like Pod and network policies to enforce your security and development standards.

Build on a secure foundation - Make sure to review and watch for communications from the project teams regarding any dependencies used in applications. When they patch their software, you'll need to integrate those changes in order to reduce the risk to your application.

There are multiple points of vulnerability which must be addressed to assure the security of containers and their microservice payloads.

Use a container image scanner to verify that your containers don't contain any malware or other known vulnerabilities, exposed secrets, as well as sweep for custom indicators of compromise (IoCs). This allows you to mitigate any risk before developing further or deploying to production.

Secure Your Build Pipeline

A thorough and consistent access control scheme is a must. Ensuring that only authorized users can access code repositories, integrate branches, and trigger builds that get pushed to production is a critical step to safeguarding the integrity of your pipeline.

Secure Your Application

Code should follow best practices in order to increase quality. Most security vulnerabilities are a result of simple mistakes or poor design choices. Focusing on code quality always pays security dividends. Use runtime self-protection controls to surface and identify security vulnerabilities and issues in specific lines of code. This helps close the gap during root cause analysis and leads to better overall security outcomes.

Securing Your People

There are two classifications of personnel you must consider and plan for; those that are assigned to manage and provide cybersecurity to the organization and those who are not.

The primary challenge in terms of cybersecurity personnel is the sheer shortage of qualified candidates. Four out of five hiring managers report concerns about finding people with the required skills. Many are turning to a strategy of training their existing staff.

Once hired, the next challenge is keeping security personnel challenged! If they're successful their job soon becomes a maintenance routine keeping what they've built running. This gets old quickly so management needs to continuously be finding new projects and roles to keep each employee stimulated and engaged.

Users, as we've observed already, are the most vulnerable component of any network. Unlike digital devices their responses will be varied, and unpredictable. They may miss things or make mistakes. As such, the only solution available is constant re-iteration of training on the best practices and processes involved in protecting the organization's valuable data assets.

Innovative developers are applying AI to human exposures such as phishing messages, prescreening them to improve the odds of catching phish.

Involve Experts

By now the complexity of an effective cybersecurity plan is very clear to you. Each layer of the ISO-OSI model is a science unto itself and determining best security policies for each requires some expertise in that science.

Your friends at New Horizons can recommend excellent experts at every level, but perhaps more important is to recommend that you approach the development of your cybersecurity plans, processes, policies, and procedures very seriously.

In this case, **a failure to plan may become a plan to close your doors.**

Get in touch today with an expert to assess the strength of your cybersecurity plan →

New Horizons®
Computer Learning Centers