Return to the VPLS Blog

Blog Post

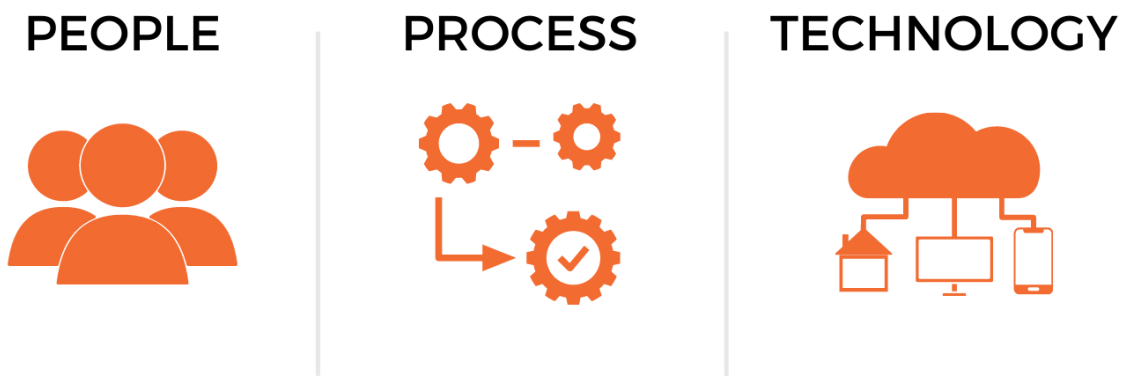
A Holistic Approach to Finding and Fixing Cybersecurity Gaps

Published
May 6, 2021

Written by
John Headley

Filed under
Cybersecurity

Cybersecurity is complex, and this is because technology itself is complex. For example, hosting and effectively protecting a public-facing web application requires knowledge of networking, firewalls, operating systems, web servers, databases, and endpoint protection software. However, the other reason that cybersecurity is complex is that security doesn't just come down to technology. Cybersecurity consists of three pillars: people, processes and technology.

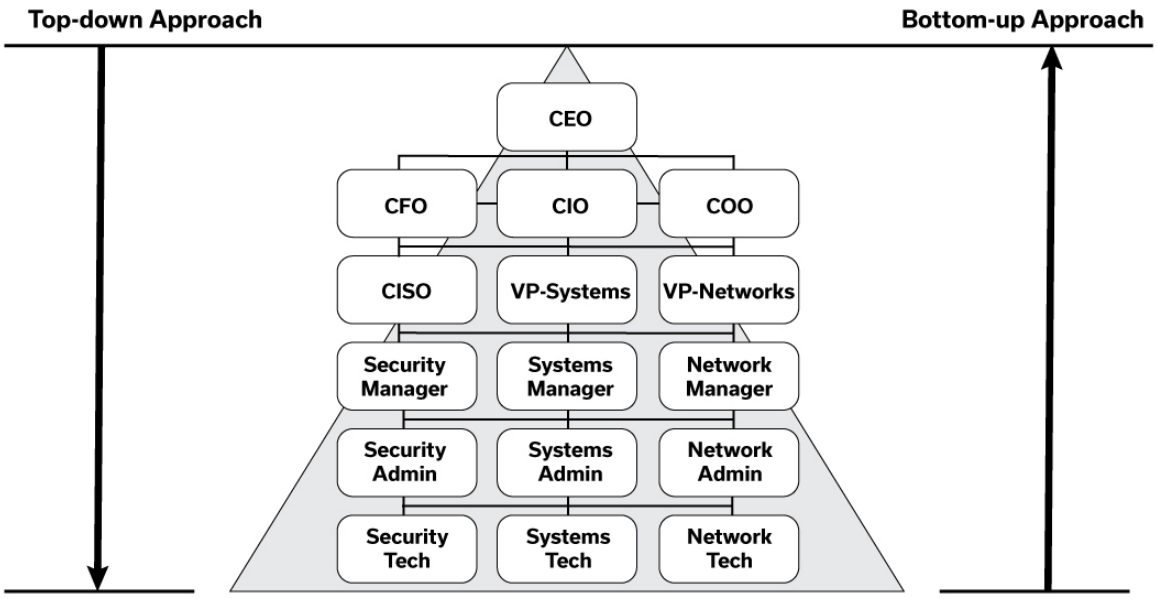


For instance, let's take an organization with skilled engineers who ensure their firewall rules are locked down and configured according to best practices. However, in this scenario, the organization doesn't patch the firewall regularly, and a threat actor exploits a vulnerability in old firmware (I'm looking at you CVE-2018-13379). In this case, the lack of processes caused the data breach, not the absence of technology.

Top-Down vs Bottom-Up Approach

Often our clients have engineers who know a lot about security. Their engineers may understand the difference between Telnet and SSH, the difference between regular endpoint protection and EDR, or the difference between SSL certificate inspection and SSL decryption. We even have clients that have checked off all the boxes on our How to Prevent Ransomware list yet still have cybersecurity gaps. Why?

This issue arises when engineers drive an organization's security program. Having one person or even one team that does not know everything there is to know about cybersecurity is not positioning an organization for success. More often than not, engineers will only focus on technology and technical controls, often reactively instead of proactively, ignoring the pillars of people and processes.



An effective cybersecurity strategy is to use a top-down approach instead of a bottom-up, engineer-driven approach. In a top-down approach, the security program is driven by executives, and mainly by a security authority within the organization, such as a Chief Information Security Officer (CISO). This authority measures the company against a master checklist of items. It then delegates the lower-level analysis and requirements to the other managers and their engineers who can interpret and implement the necessary security controls.

What master list does this security authority measure the company against? An industry-standard cybersecurity framework.

Cybersecurity Frameworks

As we discussed above, one person or team within the company does not have the time, authority, or even likely the expertise to single-handedly ensure your organization's security controls are up to par. When it comes to these industry-standard cybersecurity frameworks, a consortium of security experts, with their

combined expertise and diverse, real-world experience, have come together to think of everything an organization should think about when it comes to security. The result is a comprehensive, holistic set of requirements and/or recommendations spanning people, processes, and technology.

An example of the structure of a framework called the Center for Internet Security (CIS) Controls is shown below.

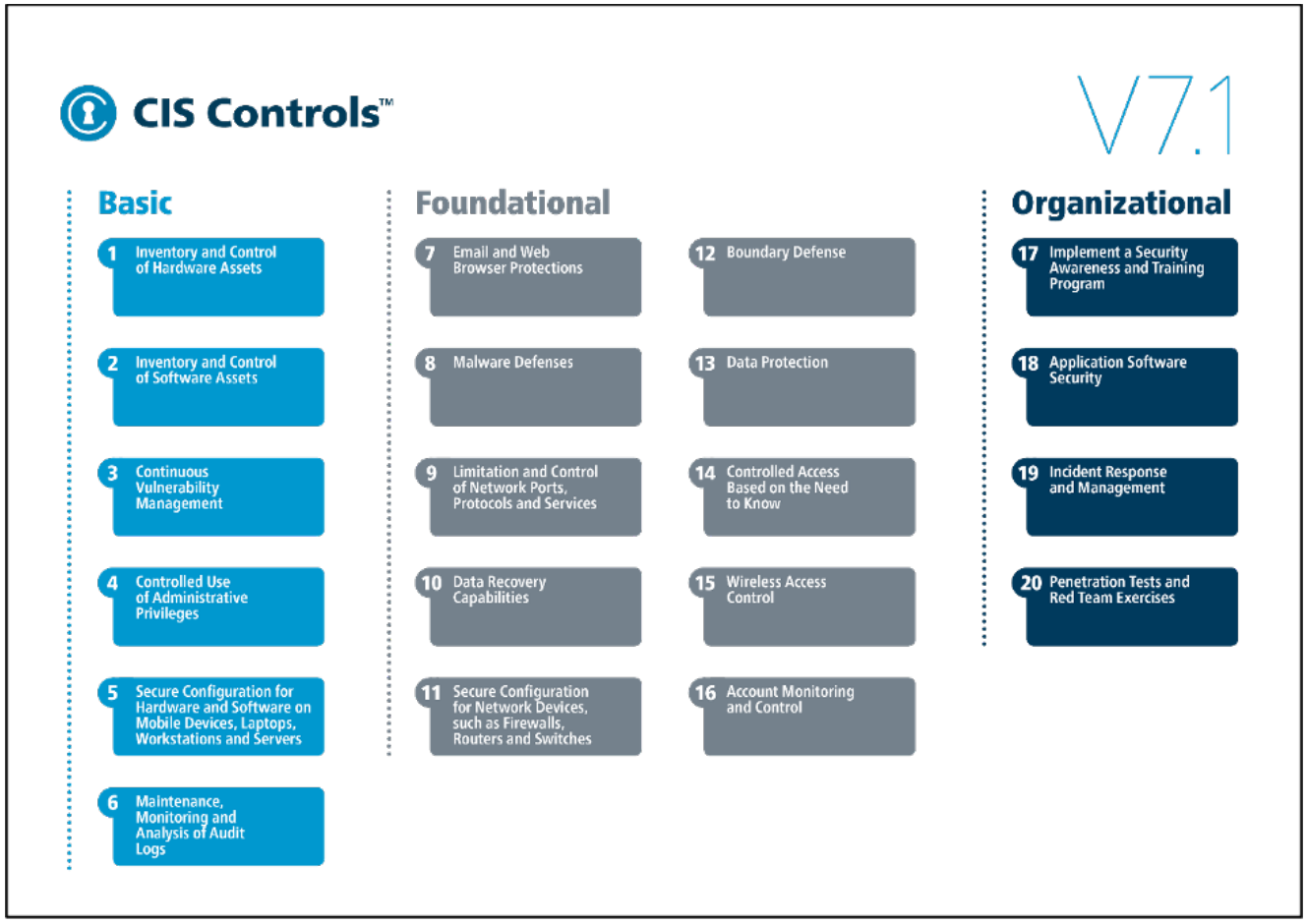


Image source: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-cis-controls/

It should be noted that there are a few subcategories of cybersecurity frameworks available. These subcategories are control frameworks, program frameworks, and risk frameworks, and the general advice is that, as an organization matures, they adopt one or more of each of these types of frameworks. Although we won't get into the weeds in this blog post on the differences, some frameworks for you to explore of each type are shown below.

Control Frameworks	Program Frameworks	Risk Frameworks

NIST 800-53	NIST CSF	NIST 800-39, 800-37, 800-30
CIS Controls	ISO 27001	ISO 27005
		FAIR

Adopt a Framework Today

Our recommended way to holistically find and fix all possible gaps within your security posture is to evaluate your organization using an industry-standard cybersecurity framework. And not just once – the organization should be continually evaluated against this framework, and a cybersecurity leader within the organization should drive the security program using this framework in a top-down approach.

If your organization doesn't have a CISO or other similar security authority, or if it does but, you would like assistance getting started with a cybersecurity framework, please reach out to us. VPLS can provide virtual CIO (vCIO) and virtual CISO (vCISO) services, including cybersecurity program reviews and security assessments, to help get your organization off to a running start with a new, holistic approach to cybersecurity.

Read More from this Author

John Headley

John Headley, CISSP and Fortinet NSE8 #003155, is a Senior Security Engineer at VPLS where he splits his time between both pre-sales and post-sales engagements. His expertise is in security architecture and engineering, security assessment and compliance, and security operations. During his time at VPLS, he has led many security-related professional services projects, including a 35-location international firewall deployment for a publicly-traded social media company.

More from this Author

PREVIOUS
VPLS is Now A CMAS Partner for Ruckus CommSc...

NEXT
ASUS Cloud, a division of ASUS, selects VPLS for a ...

If you enjoyed this article, you'll probably like:

5 Reasons SOC-as-a-Service Features Help You

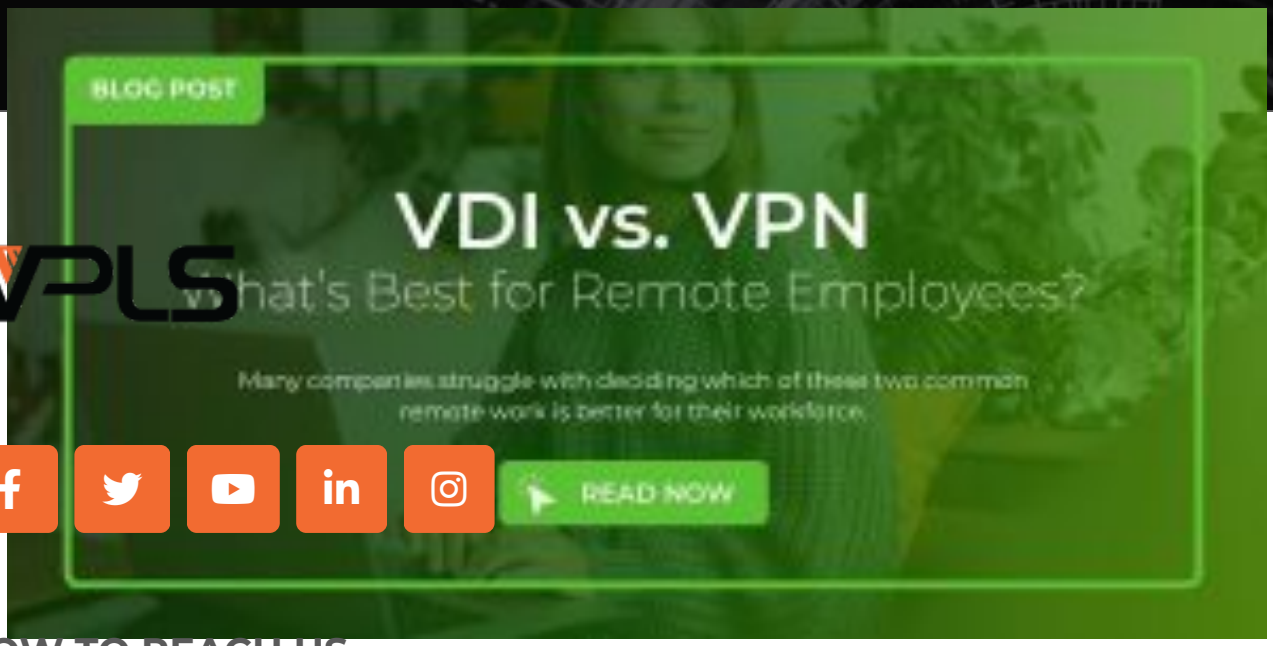
March 29, 2022

Read More »

What Is SOC-as-a-Service?

March 28, 2022

Read More »



VDI vs. VPN: What's Best for Remote Employees?

March 28, 2022

Read More »

HOW TO REACH US

Corporate Headquarters

600 West 7th Street, Suite 510
Los Angeles, CA 90017

24/7/365 Customer Service

+1 (888) 365-2656

support@vpls.com

Sales Inquiries
+1 (888) 365-2656
sales@vpls.com

WHAT WE DO

Cloud
Hosting
Colocation
Network Services
Managed Services
Professional Services
VAR

WHO WE SERVE

Financial Services
Healthcare and Life Sciences
Media & Entertainment
Telecom
Startup
Enterprise
Public Sector