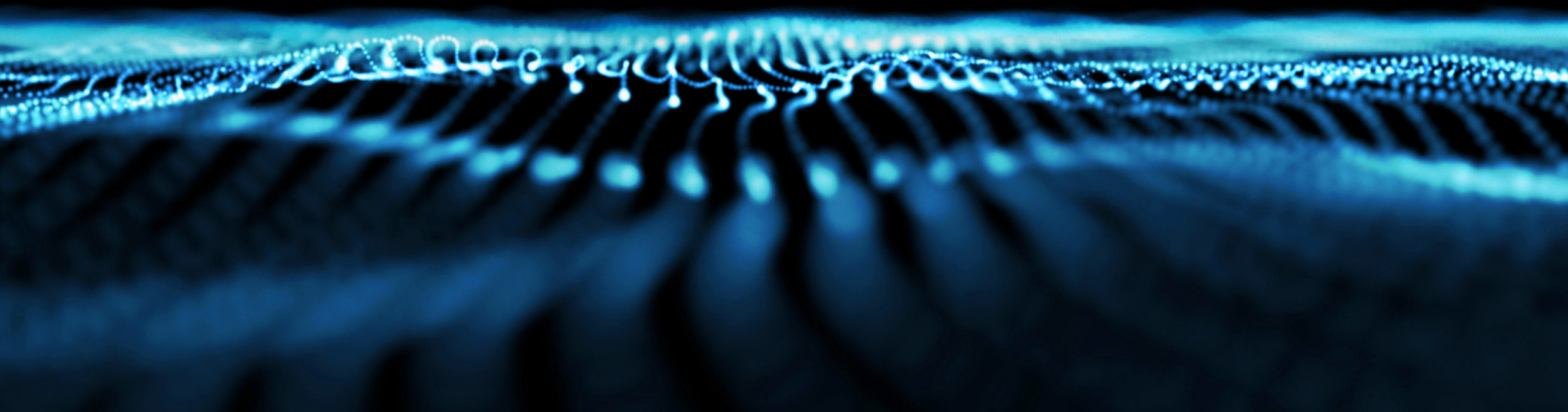
CYTELLIX

CYBER ESSENTIALS SERIES

More 6^WAYS TO STRENGTHEN YOUR CYBERSECURITY

eBook



INTRODUCTION

PROTECTION STARTS IN YOUR OWN ENVIRONMENT

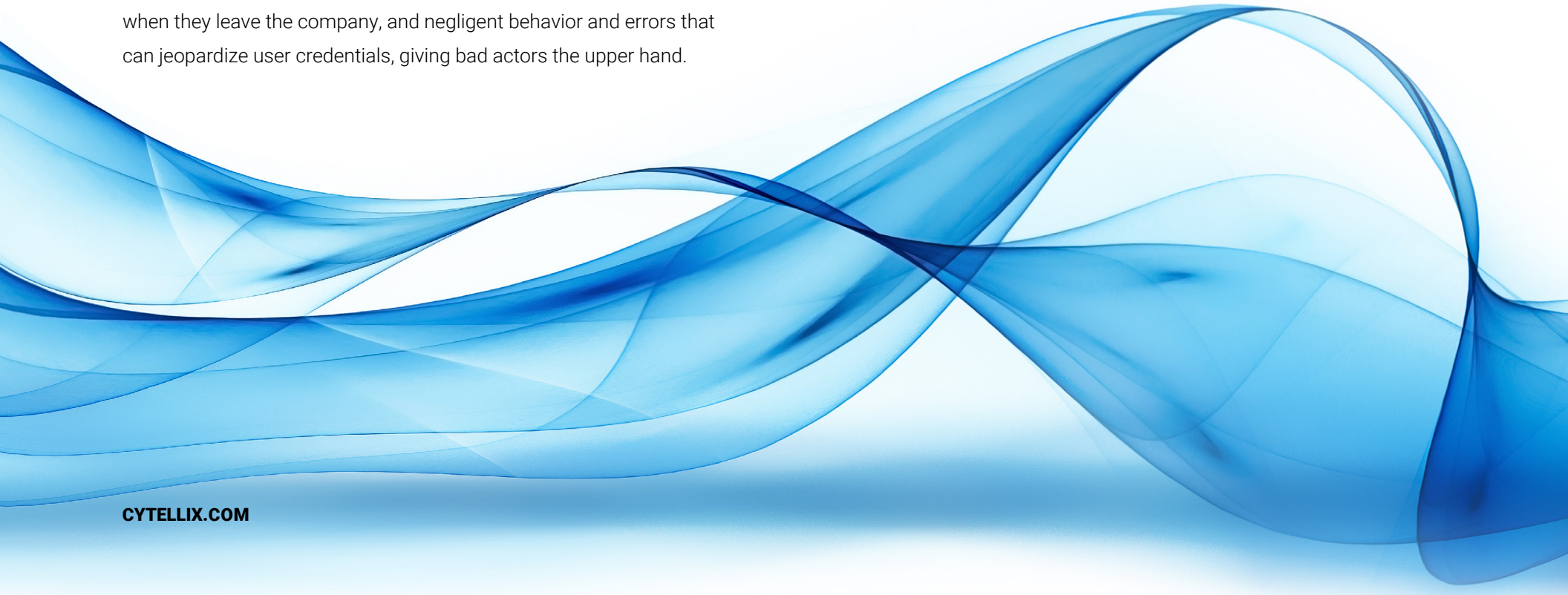
TAKE CONTROL OF YOUR CYBER RISK

Your modern security team has the nearly impossible task of protecting your organization's digital ecosystem as it expands to the cloud, third parties, and remote workforces. Not only are the risks in these environments largely hidden, they also are outside the influence of your corporate security policies and controls.

And external risk is only one part of the equation. Intentional or not, employees pose a meaningful danger to the organization. Insider risk examples include employees taking sensitive corporate data with them when they leave the company, and negligent behavior and errors that can jeopardize user credentials, giving bad actors the upper hand.

While some of these scenarios may fall outside of your purview, there are aspects that your team can control, enabling you to harden your cyber defenses and proactively reduce your overall risk. Efforts include practicing proper system and software hygiene, implementing regular testing, and securing often-overlooked portable media assets.

Ready to make take control of the risks you face? Keep reading to discover **6 ways** you can start strengthening your organization's cybersecurity today.



IS AN OUNCE OF PREVENTION REALLY WORTH A POUND OF CURE?

SECURITY TIP #1

KEEP YOUR TECHNOLOGY HEALTHY

DON'T IGNORE THE MAINTENANCE BASICS

WHY:

Your business relies on the IT assets, systems, and software applications that support it. Regular maintenance keeps your technology operating at peak performance and can catch issues before they result in unexpected downtime or failures that could impact your operations. Certain maintenance activities also may be required under warranty. Though less regular, timing-wise, maintenance also includes vendor updates to technical capabilities and software patches to fix bugs and security gaps that may make an asset susceptible to exploitation.

HOW:

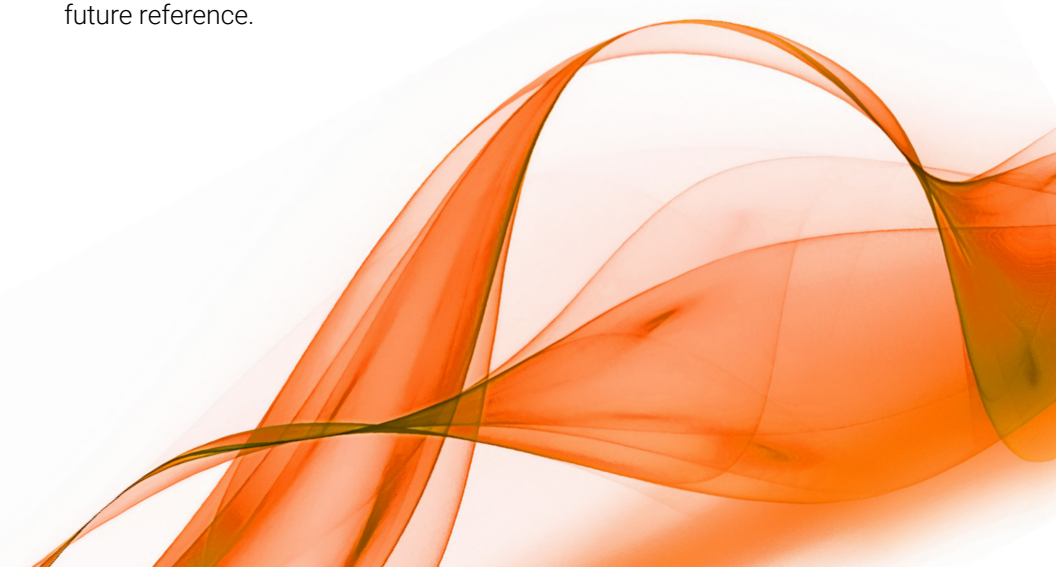
There is no "standard" cadence for maintenance since several factors can influence its timing, such as corporate policy, compliance obligations, service level agreements (SLAs), and resource availability. One of the benefits of regular maintenance is your ability to plan when it occurs, for instance, during off-hours so that any downtime does not impact business operations.

Security should be top of mind during these activities that can occur onsite or at an offsite location. You (or a person you designate) should authorize, monitor, and control all maintenance and repair activities.

Before removing an asset from your facility for offsite maintenance or repairs, sanitize the asset so that no information resides on it while it's out of your hands.

Ensure that those performing remote service or diagnostics on your asset have the required access authorizations – or appoint an internal resource that does – and utilize strong identification and authentication techniques. Test diagnostic programs for malicious code before they are used on your assets.

Following maintenance or repair, check to verify that all potentially impacted security controls are still functioning properly, terminate all remote sessions and network connections, and document all activity for future reference.



WHERE DO YOU KEEP ALL YOUR VALUABLES?

SECURITY TIP #2

IF YOU BUILD IT, THEY WILL COME

BUT LIMIT ACCESS TO YOUR MEDIA LIBRARY

WHY:

"Least privilege" is the concept of assigning permissions only to those corporate systems, data files, and applications users need to do their jobs. This role-based access minimizes the risk of accidental data exposure and privilege misuse and limits the damage if a user's credentials are compromised. For the same reasons, these restrictions should extend to your digital and non-digital media (external/removable hard disk drives, flash drives, compact disks, diskettes, digital video disks, paper, microfilm, magnetic tape).

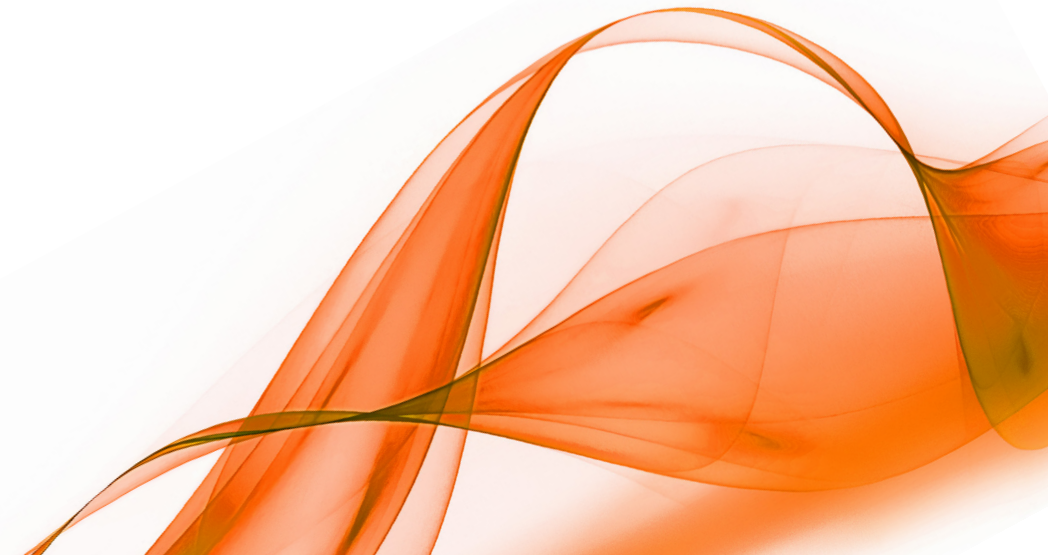
HOW:

The physical attributes of digital and non-digital media types require a physical approach to managing their access. Establish a media library – a controlled area that houses your organization's digital and non-digital media – and set corporate policies for the media types that must be stored there.

Inventory your media assets, assign permissions for media access based on user role, and set check-in/return procedures that enforce accountability and document activities associated with the transport of media outside of controlled areas.

These efforts protect sensitive information system media until it is sanitized based on your organization's records retention policies and using corporate-approved equipment, techniques, and procedures. Sanitation removes information from the media so that it cannot be retrieved or reconstructed when the media is reused or released for disposal.

Ensure that the sanitization techniques – including clearing, purging, cryptographic erase, and destruction – correspond with the security category classification of the information stored. Media sanitation should be carefully documented, and dual authorization required to ensure that two technically qualified individuals conduct the task.



DO YOU HAVE AN EXIT PLAN?

SECURITY TIP #3

GRANTING AND REVOKING INSIDER ACCESS ARE EQUALLY IMPORTANT

DON'T LEAVE DOORS OPEN TO RISK

WHY:

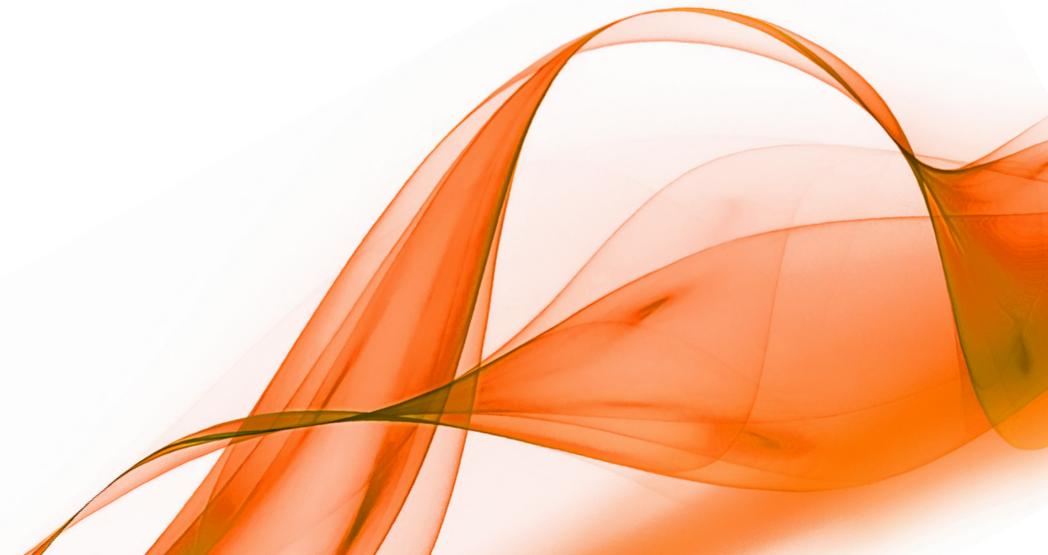
Any time you allow access to your systems, you risk misuse, whether it's intentional or not. Insider risk is real, and with legitimate credentials, it's easy for a user with malicious intent to gain – or provide – unauthorized access to corporate data. User negligence also is a risk. It's important, therefore, to carefully manage use cases such as exiting employees, and have defined policies and procedures for assigning – and revoking – access to systems, data files, and applications.

HOW:

As we mention in Tip #2, following the "least privilege" concept and applying role-based access permissions will help minimize insider risk. Assign a risk designation to each role based on the type and sensitivity of assets and information the role will need access to. This will help you establish screening criteria for an individual prior to authorizing access.

Defining the set of policies and procedures involved in revoking user access is just as vital. Use cases include employee transfers or role reassignments within your organization and employee exits/terminations.

In all cases, disable all information system access authorizations associated with that user, reclaim all corporate-owned devices, and retrieve physical security-related property such as building keys, passes, and identification cards. Reissue the appropriate physical and information system access to employees who are being transferred or reassigned within your organization based on their *new* role.



ON A CLEAR DAY, CAN YOU SEE ALL YOUR RISKS?

SECURITY TIP #4

RISK EXISTS ACROSS YOUR ENVIRONMENT

GET A BETTER VIEW

WHY:

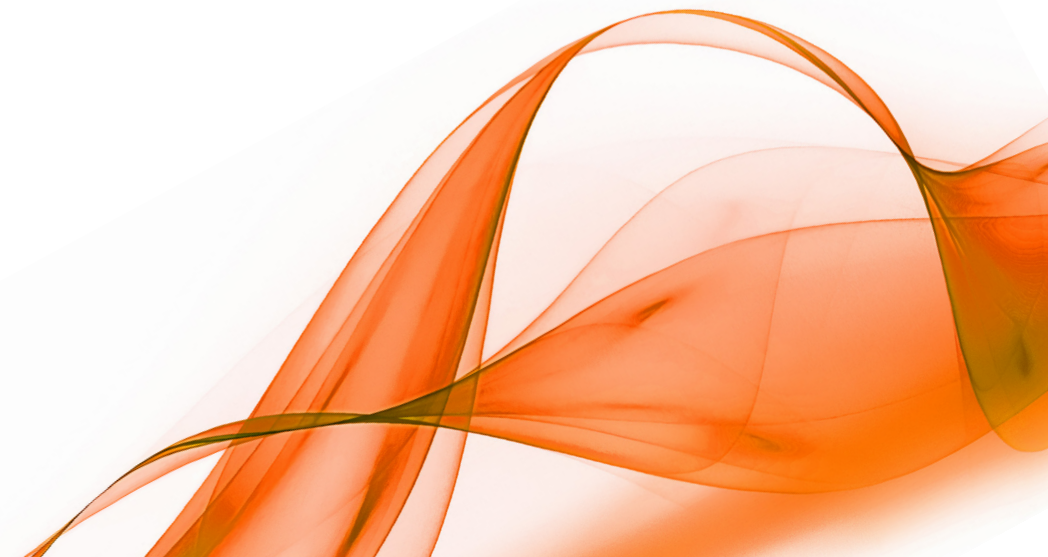
Where your assets reside (on-premise, in the cloud), whether you use third parties, and who and what devices have access to your systems are among the factors that determine your company's level of risk. The ability to visualize risk across your entire attack surface is essential, including the vulnerabilities that exist, their exploitability, and the potential impacts to your business from unauthorized access, asset disruption, or information disclosure or destruction.

HOW:

You can gain a critical view of the risks you face – and their likelihood of impacting your business – by conducting a risk assessment of your environment. Risks can be inherent to your business type, industry, IT/OT infrastructure, and even the external service providers, partners, and contractors you work with.

Scanning tools can flag known vulnerabilities that exist in your environment, giving you the chance to proactively address those that pose a danger to your business *before* they can be exploited. Tools can scan for patch levels, functions, ports, protocols, services, and for improperly configured or incorrectly operating information flow control mechanisms. Ensure that all potential sources of vulnerabilities are included in the scans, such as information system components, networked printers, scanners, and copiers.

Choose tools that rank vulnerabilities according to their severity using the Common Vulnerabilities and Exposures (CVE) naming convention, and that use the Open Vulnerability Assessment Language (OVAL) to determine and test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).



HOW WELL IS YOUR CYBERSECURITY PROTECTING YOU FROM RISK?

SECURITY TIP #5

TAKE STEPS TO BOOST SECURITY PERFORMANCE

SMALL ADJUSTMENTS CAN MAKE A BIG DIFFERENCE

WHY:

Once considered a technology function, cybersecurity's increasing role in organizational accountability has made it a business imperative. The now corporate-wide responsibility of risk management pulls measurement from IT and security teams to determine the organizations' cyber-preparedness, threat management, and the effectiveness of in-place security controls.

HOW:

Security controls refer to the technical (firewalls, software, infrastructure), physical (hardware, IP phones, IoT and OT capabilities), and operational (training, process, procedures) measures that are implemented to protect your organization's information systems and assets from cyber risk.

Because your information systems and the environments in which those systems operate change frequently, assess security controls on a regular basis and whenever changes are made to your IT infrastructure or business. Validate that controls are implemented correctly, operating as intended, and effectively meeting your established security requirements. In addition, real-time monitoring of security assets, their cyber posture, and their behaviors are critical steps in determining risk.

Knowledge is vital in terms of which services, software, connections, and environments are allowed to connect to your company infrastructure. The unknown (Shadow IT, remote environments) is the focus of risk. Consider implementing strategies to reduce risk – for instance, blacklisting allows all connectivity and denies by exception, and (stronger) whitelisting denies all and allows by exception.

Evaluate access security controls, too. For instance, ensure authorized and privileged access to information systems is being maintained (adding/removing individuals as required), output devices (printers, copiers) are in secured areas and are not leaking data to bad actors, all physical access points are monitored 24/7, and visitor policies are in place and being enforced.

Develop a plan of action and milestones to correct any identified security control weaknesses and reduce or eliminate known vulnerabilities in the system.

NEED A LITTLE HELP TO KEEP YOUR ENVIRONMENT SAFE?

SECURITY TIP #6

LEAN ON TECHNOLOGY TO ZERO IN ON THE ISSUES THAT REALLY MATTER

THE RIGHT TOOLS MAKE LIGHT WORK

WHY:

As we mentioned in Tip #1, patching is a maintenance activity that's vital to keeping your environment safe, since these vendor releases typically remediate security gaps and other flaws in software and firmware. But even as you patch one security gap, opportunistic hackers are looking for other easy entry points. Which is why you need to continuously protect and monitor your environment.

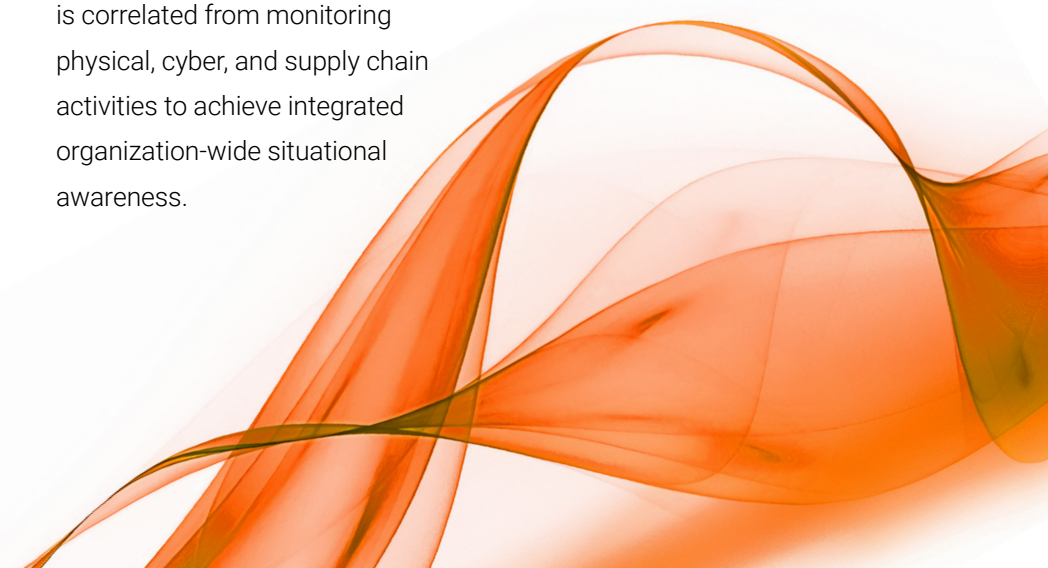
HOW:

Use technology to streamline and focus your security efforts. Protection at information system entry and exit points, for instance, can help you detect and eradicate malicious code mechanisms. These can include antivirus signature definitions and reputation-based technologies. Central management of these protections allows you to easily implement, assess, authorize, and monitor them.

Various tools and techniques can be leveraged to monitor your information systems, for example, intrusion detection and prevention systems, scanning tools, and network monitoring software.Security Information and Event Management (SIEM) tools consolidate security data feeds from sources across your environment and generate alerts and/or notifications that your team can monitor and analyze to detect attacks, indicators of compromise, and unauthorized connections.

Automated tools and technologies assist your team in examining inbound and outbound traffic for unusual or unauthorized activities or conditions, such as large file transfers, persistent connections, unusual protocols, and ports in use. They can also alert security personnel of inappropriate or unusual (or suspicious) activities that could indicate potential security risks such as insider threats.

A wireless intrusion detection system identifies rogue wireless devices and detects attack attempts and potential compromises. Information is correlated from monitoring physical, cyber, and supply chain activities to achieve integrated organization-wide situational awareness.



CONCLUSION

QUICK STEPS TO A BIG IMPACT
TAKE CONTROL OF THE RISKS YOU FACE

As your digital ecosystem expands, so does your attack surface. But in cloud, third-party, and remote environments there's only so much risk you can manage.

It's why good security must start in your environment.

Follow the proactive tips we outline in this guide to start strengthening your cybersecurity (find *6 more quick tips* in part one of this Cyber Essentials Series). And if you need a partner to guide or supplement your security efforts, Cytellix is here to help.

We offer multiple levels of GRC, MDR, and XDR services based on our integrated stack of leading technologies. Our on-demand services and skilled cybersecurity experts make strengthening your cybersecurity posture effortless and immediate.

SEE FOR YOURSELF HOW CYTELLIX CAN STRENGTHEN YOUR CYBERSECURITY

SCHEDULE A DEMO

CYTELLIX

cytellix.com

info@cytellix.com

(949) 215-8889