CYTELLIX

CYBER ESSENTIALS SERIES

6 WAYS TO STRENGTHEN YOUR CYBERSECURITY

eBook

INTRODUCTION

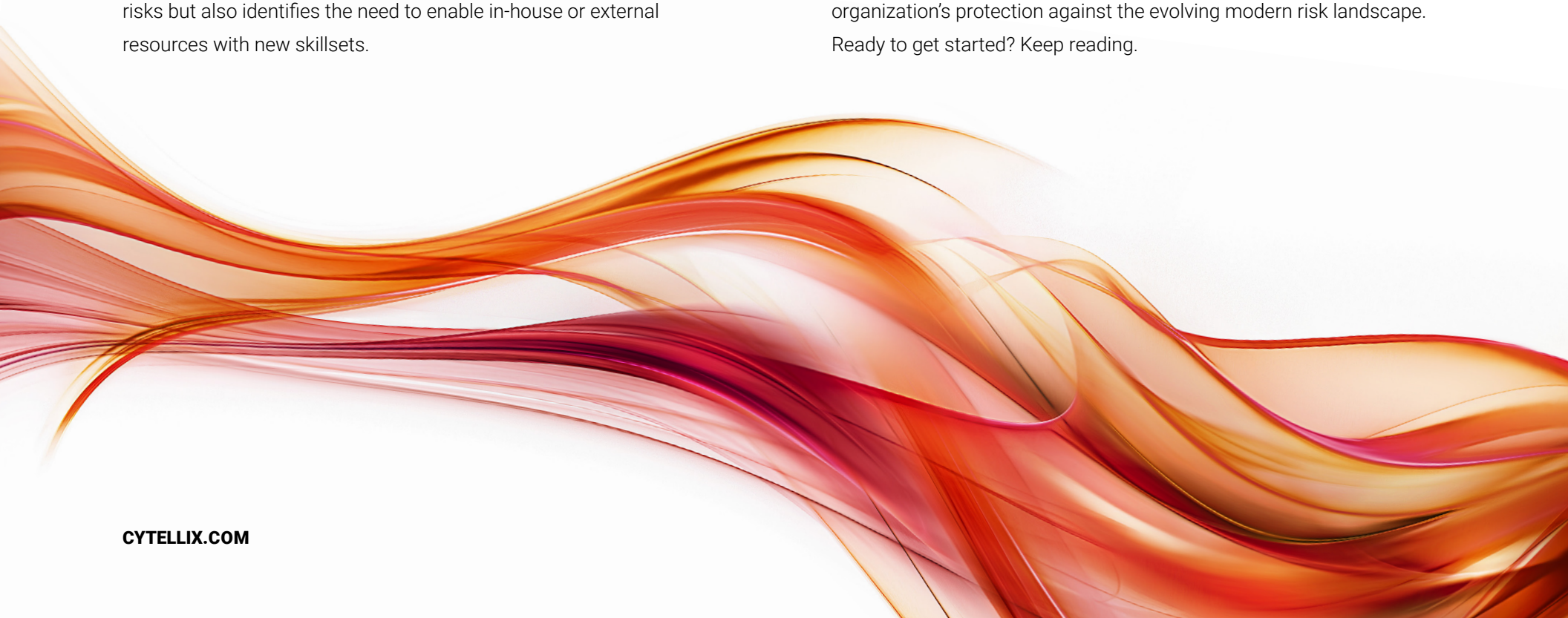
DON'T JUST TAKE SHOTS IN THE DARK
UNDERSTAND YOUR CYBERSECURITY RISK

From the data center to the cloud, today's distributed environments extend opportunities for businesses. As access to innovative technologies drives operational efficiencies, optimizes worker productivity, and broadens corporate reach, it also introduces risk.

Cybersecurity, therefore, plays an increasingly critical role as organizations extend their environments. Its consideration as part of an innovative business approach creates an environment to eliminate risks but also identifies the need to enable in-house or external resources with new skillsets.

Enablement, though, is not without its obstacles, particularly for in-house efforts. For instance, finding and retaining specialized resources needed to manage advanced security tools can be challenging amid a global talent shortage. And while security point solutions address specific security issues, they leave significant gaps in protection.

The good news? A strong cybersecurity program doesn't have to be out of reach. Inside this guide, we outline **6 ways** to boost your organization's protection against the evolving modern risk landscape. Ready to get started? Keep reading.



IS YOUR USER ACCESS OUT OF CONTROL?

SECURITY TIP #1

USER ACCESS ISN'T FOR EVERYONE

SET YOUR LIMITS

WHY:

Your users need access to applications and systems to do their jobs effectively – from wherever they are and from whatever device they're using. This doesn't mean all users need equal access. The marketing department doesn't need access to sensitive financial records or client payment information for instance. Defining access based on a user's role helps limit unnecessary access to systems and information, and therefore limits risk if a user's credentials are compromised or in the case of insider threats.

HOW:

Use a combination of administrative and technical controls to set limits and manage user access.

Administrative controls include policies that control access to applications and systems for multiple use cases including BYOD, remote workers, or rules-based. Align access policies with your organization's compliance obligations for protecting sensitive information. Monitor access for unusual activity or changes including physical and behavior changes, new users and devices, and more.

Technical and logical controls leverage technology and automation to protect access. For instance, use these controls to limit the number of users who can access your applications and systems. Implement two-factor or multi-factor authentication to protect access – and choose an option that balances user experience and security. Set policies for the number of logon attempts before an account is automatically locked, idle time and logon time before a session is suspended, define password length and strength (see Security Tip #5), and device protection such as antivirus or endpoint detection software and manage via a centralized system. Use a next-generation firewall that inspects network traffic at both the packet and application levels and block all traffic by default except specific traffic to known services.

ARE YOU ABLE TO LOOK IN THE REARVIEW MIRROR?

SECURITY TIP #2

THE CLUES TO SKETCHY USER ACTIVITY ARE IN THE PAST

RETRACE THEIR STEPS

WHY:

The ability to retrace access to files, applications, and systems is helpful for tracking down unauthorized activity following a breach. Audits also often are mandated by compliance regulations depending on your industry. Be ready for both by establishing policies and configurations to capture critical access history.

HOW:

The right data enables you to monitor, analyze, investigate, and report any unlawful, unauthorized, or inappropriate information system access or activity. Configure your information systems to capture helpful data points, such as user logins, IP addresses, machine addresses, system names, and dates and times. Audits may have additional data-capture requirements such as server startup and shutdown, system alerts, user logon/logoff, and data that establishes the occurrence, sources, and outcomes of events.

For both general accountability and audits, records should utilize the Network Time Protocol (NTP). This ensures that logs – organization-wide – are synced with the same time source. Plus, ensure sufficient storage capacity for your records – particularly when needed for compliance and audits.

Leverage technology to automate audit record review and for alerting the appropriate roles for critical issues, such as audit failure or when storage capacity is almost full. Train all staff tasked with log management responsibilities on how to review and analyze audit logs and report incidents. Security is essential too, so ensure that audit data and tools are protected, retained, and backed up according to your compliance obligations and/or corporate policy.

WHO'S THE WEAKEST LINK IN YOUR SECURITY CHAIN?

SECURITY TIP #3

GIVE USERS THE TOOLS TO PROTECT THEMSELVES (AND YOU)

TEACH YOUR USERS WELL

WHY:

Users are the weakest link in your security chain. More than 95% of security breaches are the result of human error[1], such as clicking on a phishing email or misconfiguring a critical system. Strengthening your users' knowledge and awareness of risk serves to strengthen your security. Provide regular and basic security awareness training to existing information system users (including managers, senior executives, and contractors), and establish training as a part of new employee or new-user onboarding and as required by information system changes.

HOW:

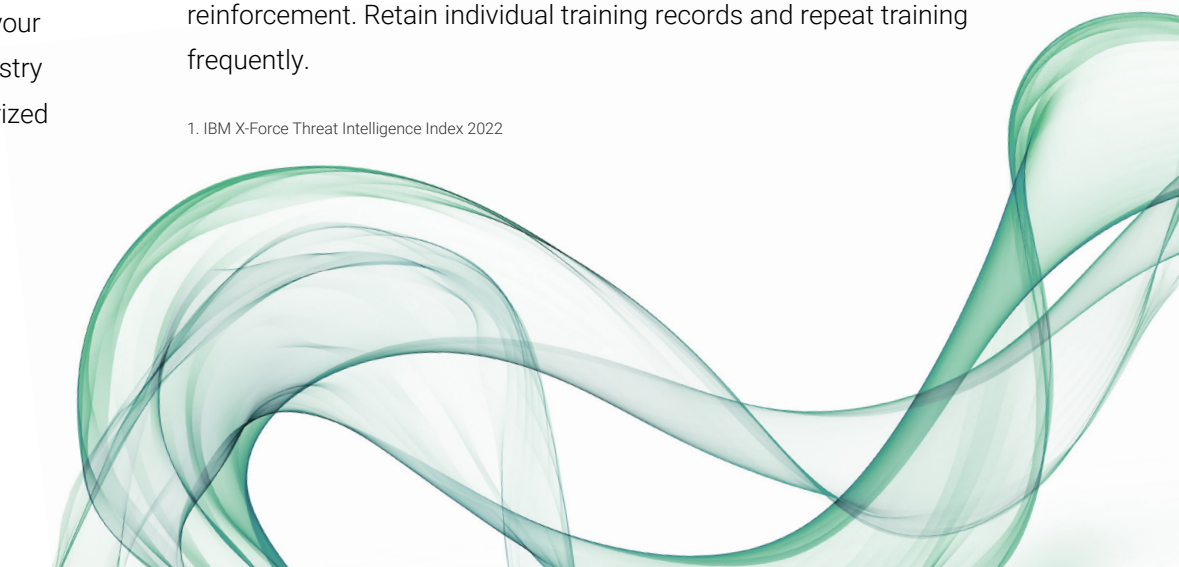
Training forms a good foundation for building employees' security awareness. Customize the content, techniques, and frequency of your training based on your specific needs, such as organizational/industry requirements and the information systems your users have authorized access to.

In general, the content of your training should develop your users' understanding of the importance of security, user behaviors that maintain – or hurt – security, potential indicators of insider threat, how to recognize suspicious email communications, and how (and to whom in your organization) to report suspected security incidents.

Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Document and monitor your security training activities, including basic security awareness training and specific information system security training to identify any red flags or topics that may require reinforcement. Retain individual training records and repeat training frequently.

1. IBM X-Force Threat Intelligence Index 2022



ARE YOU LEAVING DOORS OPEN FOR CYBERCRIMINALS?

SECURITY TIP #4

ESTABLISH THE GROUND RULES FOR CONSISTENCY AND SECURITY

CONFIGURATION MATTERS

WHY:

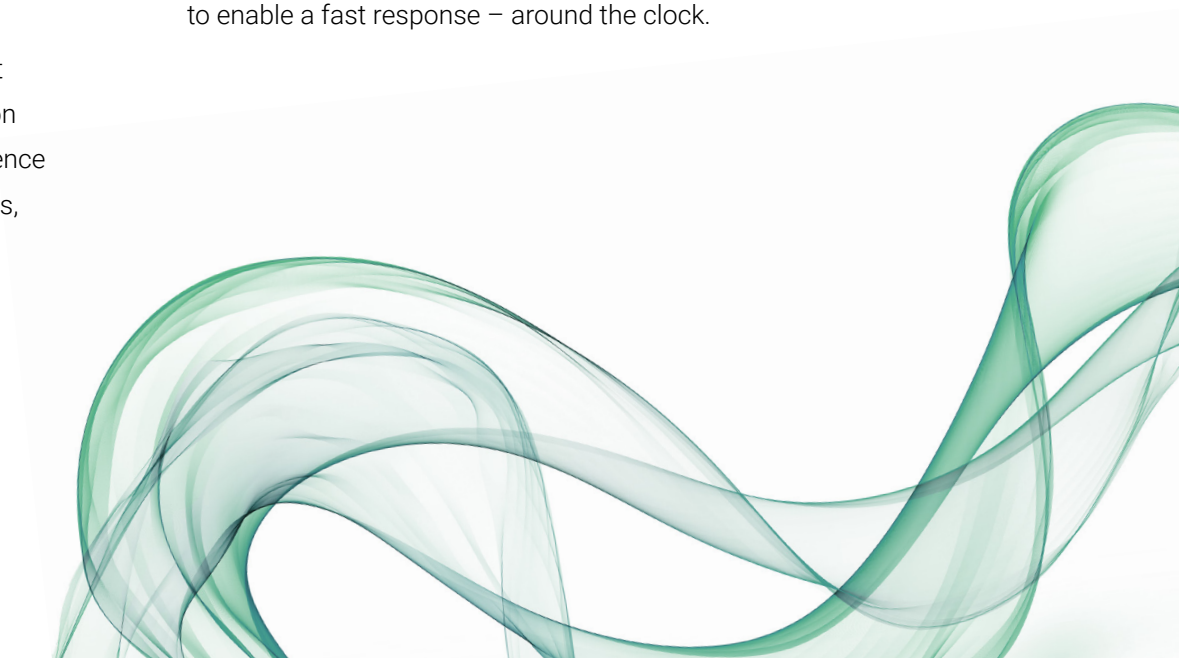
Configuration errors in machines, systems, software tools, and applications can expose those assets. It's like leaving the door open for criminals who are looking for easy access to your information. A well-defined configuration management process will help you minimize configuration errors and actively reduce the number of exploitable gaps in your environment.

HOW:

Like most efforts, ensuring proper configuration in your environment begins with establishing some ground rules. Define the roles responsible for configuration management in your organization; identify the tools, resources, and facilities that will be used; and set and document configuration standards, testing and implementation procedures, and guidelines for project or IT teams to follow. Reference and/or include specific compliance guidelines, such as DISA's Ports, Protocols, and Service Management (PPSM) instructions, when developing these supporting resourcets.

Configuration changes can disrupt operations or trigger unexpected results. Whenever possible, apply configuration changes in a test environment and analyze the security impact of the changes prior to implementation in your production environment. Implement changes after hours to reduce any impact on business operations.

Minimize your attack surface by configuring to the principle of least functionality – in other words, allow only essential capabilities. Restrict, disable, and prevent the use of unnecessary programs, functions, ports, protocols, and services. And leverage technology to automate sending critical alerts to designated responsible roles' email and mobile devices to enable a fast response – around the clock.



PSST! WHAT'S THE MAGIC WORD?

SECURITY TIP #5

PROTECT THE KEYS TO YOUR KINGDOM

REINFORCE SAFE AUTHENTICATION PRACTICES

WHY:

User names and passwords are the "keys" to your systems. They represent an authorized user's identity. But these credentials also are easily lost or stolen, providing an easy way for attackers to gain what can appear to be authorized access to your systems. In fact, stolen credentials are the cause of more than 60% of data breaches.[2] It's important to help users understand the importance of keeping their passwords secure – along with policies that reinforce safe use.

HOW:

Security can be challenge in this age of BYOD, remote workforce, and remote and home-based offices. Policies can help reinforce "safe" user behaviors around user identity and password use to minimize misuse or theft.

Uniquely identify users for authorized access to the appropriate systems, applications, and data based on their role. Authenticate user identities through the use of passwords, tokens, biometrics – or, in the case of multifactor authentication, some combination thereof.

At a minimum, employ two-factor authentication for all network-based access used to perform administrative functions on servers or multi-user systems, and audit access to these systems.

Set automated limits to disable user identifiers after a determined timeframe of inactivity (e.g., 30 days). Systems should require all passwords to be a minimum level of complexity and difficult for unauthorized people to guess. Set policies for password strength, (e.g., must be at least eight characters long and contain a combination of upper- and lower-case letters, numbers, and special characters). Enforce regular password changes through automation at the system-level (e.g., Windows admin and application administration accounts) and user-level (e.g., for email, web, desktop computer). And establish – and publish – your policy for users who suspect that their password has been compromised, including how to report and how to reset.

2. Verizon Data Breach Investigations Report 2021

ARE YOU PREPARED TO TACKLE AN INTRUDER?

SECURITY TIP #6

THE SECRETS TO RAPID AND EFFECTIVE INCIDENT RESPONSE

PRACTICE MAKES PERFECT

WHY:

It's important to have the ability to identify and detect a threat or suspicious activity in your environment. Once detected, a fast response can minimize the damage. An incident response plan is essential to that fast response, and includes containment/mitigation, analysis, recovery, follow-up, and the identification of specific user roles and responsibilities to carry out your response activities.

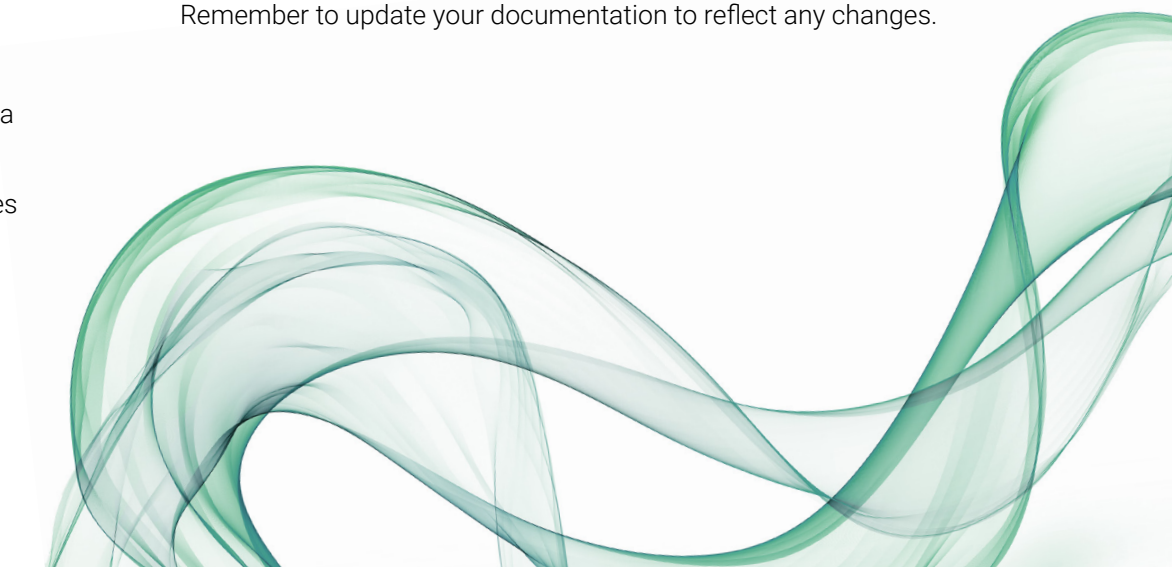
HOW:

When a cyber incident happens, the last thing you want to be is unprepared. Any delays or missteps can have serious reputational and regulatory consequences. Fortunately, it's possible to plan your response so that everyone knows ahead of time what should be done – and when.

To start, identify your incident response team and clearly establish a chain of command as well as the roles and responsibilities of each member. Ensure that the appropriate cross-organizational resources are allotted and committed.

Define a formal incident response plan that considers multiple scenarios, their implications, and the tools and actions needed to mitigate the damage. Plans often rely on key individuals. If these people are not available, a verbal plan may fail, so documenting the details of your plan is essential. A written plan also importantly serves as a steady reference amid the chaos of an active incident. Include a checklist and procedures for system shutdown, startup, and restoration. Define practices for collecting evidence and have a method to track, document, and report incidents.

Test, revise, and use drills so that the team can practice the plan regularly to ensure it works, and can be adapted if there are changes in team members, incident scenarios, infrastructures, and threats. Remember to update your documentation to reflect any changes.



CONCLUSION

TAKE STEPS TO STRENGTHEN YOUR PROTECTION AND REDUCE RISK

ADDRESS THE RISKS YOU FACE

Along with business technologies, security tools have advanced to protect against and manage modern risk.

In-house implementation and ongoing management of these technologies require budget as well as expertise and skilled resources – which are hard to come by with the current global security talent shortage.

Outsourcing security offers a viable alternative, but managed services vendors typically deliver point solutions that leave significant gaps in protection. Governance Risk and Compliance (GRC) and Managed Detection and Response (MDR) providers such as Cytellix bridge risk and security, operationalizing the people, processes, and multiple technologies needed to manage risk and detect and respond to threats quickly and holistically.

Cybersecurity is essential for any organization in today's aggressive threat landscape. Follow the tips offered in this eBook to start strengthening your protection. And if you need a partner to guide 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 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