TOOLKIT

CompTIA IT Security Toolkit

CompTIA

Introduction

This toolkit is a reference tool and body of knowledge to assist you in addressing security concerns for your business. It is designed to simplify the myriad demands of cybersecurity and/or compliance and provide starting points for continual improvement of security processes, people and technology. The guidance within this toolkit is driven by CompTIA and industry research.

By focusing on the People, Processes, Technology, and Research a sound environment for security can be created. An environment that is practical for its users, secure in its system design, and supported with proper technology and policies.

1 People

2 Processes

3 Technology

4 Research

5 Conclusion

1 People

Think of the many, many times employees are the difference between proper delivery of a service and the loss of a client. Or managing a project to successful completion versus being stuck in a death march. Time and time again, quality people are at the root of any successful business. The same is true with cybersecurity. And as with any human resource, there are ways to set employees up for success.

AWARENESS TRAINING

Identifying the right people for the right job, continuous awareness and reinforcement training, career development opportunities, and proper process controls to limit unnecessary exposure to sensitive data are all ways to empower people to play a role in maintaining a secure physical and data environment. Consider establishing a baseline of security awareness for all employees. CompTIA's research has identified 8 behaviors any employee can and should integrate into their day-to-day activities. A great way to encourage these behaviors is to provide this **INFOGRAPHIC** to your entire staff to display in their work area as a gentle reminder that their actions play a role in everyone's security.

8 Cybersecurity Commandments

1	2	3	4	5	6	7	8
Avoid doing secure work on un-secured connections	Never mix personal and work logins	Stay away from random USBs (stick drives, thumb drives, flash drives)	Don't recycle login credentials	Don't procrastinate with operating system updates	Always choose two-factor authentication	Change passwords regularly	Take advantage of cybersecurity training

Beyond the passive approach described above, the last point recommends all staff undergo a more proactive training regimen to help establish and reinforce behavior that encourages skepticism, caution, and a mental framework to choose actions that support security instead of undermine it. There are many options available to you, including CompTIA's own CyberSecure Program. Here are some resources to help align the right training for the right people.

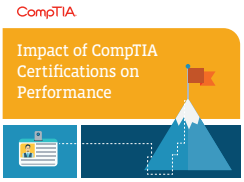
CompTIA CYBERSECURE

- **Cyber Secure:** A Look at Employee Cybersecurity Habits in the Workplace – This whitepaper examines the role and behavior of employees as it relates to cybersecurity.
- **Human Firewall Webinar:** This webinar explores how security awareness training is expanding and how to teach security awareness at these different levels.
- **CyberSecure:** CompTIA CyberSecure is a self-paced training course that teaches your employees how to follow security practices vital to protecting your business. The 60-minute training focuses on situations relevant to everyone from the receptionist to the CEO …not just the IT department.

When looking beyond CompTIA for resources, be sure to consider the mode of delivery, the outcomes you expect the training to accomplish, and the level of staff being targeted. If conducting internet searches for viable options, utilize good search terms such as: "security awareness training"; "safe internet usage"; or "on-going security awareness" to help locate a program that suits your needs.

Getting everyone on the same level is a great way to start. But as you are only too aware, privileged users, management, executives, and security personnel require additional training as they represent a higher risk when it comes to exposing the information they may be privy to.

For these higher risk positions, consider more in-depth training, specific to their risk profile and job roles. Social engineers have identified the power of adopting the persona of a manager to pressure an employee to provide information they may otherwise not turn over. Login credentials, confidential reports, and sensitive data can be leaked when an employee is trying to "do the right thing" by obeying what they assume is a legitimate request from who they assume is a legitimate executive. When in reality, neither of those assumptions are true. This is only one example of how privileged users present a unique challenge to managing risk.



SECURITY PROFESSIONALS AND CERTIFICATIONS

For staff with a role in maintaining the integrity of your data systems, it is vital they have the proper training, experience, and credentials to prove their mettle. Whether you seek out professionals with security certifications in hand or offer career development opportunities to advance people within your organization you have identified as ready for the challenge, professional security training and certification is essential for higher level/higher risk employees.

CompTIA's Professional Certifications have long been recognized as the industry standard. Your security and network professionals consider the impact of security on your devices, network, management system, and staff on a daily basis. Depending on their role, consider the following vendor-neutral CompTIA certification programs for your privileged users:

- **CompTIA Network+:** Great for job roles concerned with the design, configuration, management and troubleshooting of wired and wireless devices. Job roles such as Network Field Technician, Network Support Specialist, Network Administrator, Network Analyst, and Help Desk Technician are good candidates for CompTIA Network+.
- **CompTIA Server+:** Build, secure and troubleshoot server hardware and software technologies with staff properly trained and certified across vendor platforms. Systems Engineer. Server Administrator, Sales Solution Specialist (Servers) would find great value in the skills and knowledge validated by CompTIA Server+.

- **CompTIA Cybersecurity Career Path Hub:** CompTIA certifications help individuals build exceptional careers in information technology and enable organizations to form a skilled and confident staff. Choose the path that is right for you and get certified so you can be ready for today's and tomorrow's IT challenges.
- **CompTIA Security+:** For more advanced staff, specifically concerned with aspects of network security, this certification covers best practices in securing a wired and wireless network and managing risk. For staff with over 2 years of experience and serving in roles such as Security Architect, Security Engineer, Security Consultant, Security Specialist, Security or Systems Administrator, CompTIA Security+ is ideal.
- **CompTIA CSA+:** CompTIA Cybersecurity Analyst (CSA+) is an international, vendor-neutral cybersecurity certification that applies behavioral analytics to improve the overall state of IT security. CSA+ validates critical knowledge and skills that are required to prevent, detect and combat cybersecurity threats.
- **CompTIA Advanced Security Practitioner:** Designed for advanced security for complex environments, individuals with more than 10 years of experience in IT administration will find this certification valuable. Roles such as Information Security Analyst, Security Architect, IT Specialist INFOSEC, IT Specialist (Cybersecurity), Cybersecurity Risk Manager, Cybersecurity Risk Analyst are reserved for this advanced professional certification program.

What can you do if you want to bring in outside experience? Finding certified security professionals can be a daunting challenge so CompTIA has created Cyberstates to help analyze the size and scope of the tech work force. For more information, see below in the Research section of the Toolkit.

Beyond CompTIA's certification programs, be sure to consider vendor and partner certifications specific to the products and business solutions in place. Deep understanding of the hardware and software utilized is a great way to get the most out of the technology.

Professional Societies and Associations are another way to stay on top of the latest education, trends, and best practices for cybersecurity. Find groups that work for you and your staff and encourage their participation with the goal of staying on the cutting edge. These groups will not only benefit your individual contributors in their roles, they can also expand your partnering network and expose you to revelatory solutions to common problems.

- **CompTIA AITP:** CompTIA Association of IT Professionals (AITP) is the leading association for technology professionals, students and educators. Join us to build your professional network, strengthen your technical knowledge and soft skills, develop a personal career path, and keep current on technology and business trends. Be part of the community that continues to push technology forward, and join thousands of other tech professionals as a CompTIA AITP member.

MANAGEMENT AND EXECUTIVE TRAINING

CompTIA offers education to help maintain security controls, targeted at the executive level. Given their higher public profile and internal influence, executives should understand their unique role in maintaining a secure environment.

These Executive Certificate courses provide in-depth training on the intricacies of managing security controls for an IT organization.

- **Executive Certificate in IT Security Foundations:** Learn to make professional risk and threat assessments, and communicate the costs of incidents before they happen, using the same tools U.S. government agencies use.
- **Executive Certificate in Business Continuity and Disaster Recovery:** The best business continuity and data recovery services have already evolved into forms of art. Learn to provide resilience, assurance, and continuity as services.

And these self-paced guides provide information at your fingertips for helping to shape a sound cybersecurity program for your organization.

- **Quick Start Guide to Security Compliance:** New government regulations on reporting and accounting are making organizations revisit their IT infrastructures. Learn how you can take advantage of this opportunity.
- **Quick Start Guide to Tackling Cloud Security Concerns:** Businesses have concerns about moving their resources to the public cloud. Sometimes those concerns stop them cold. Find out how to avoid the cloud security trap.
- **Quick Start Guide to Business Continuity and Disaster Recovery:** Learn the six steps to constructing the optimum business continuity and disaster recovery plan, for your company and for your customers. Stay resilient in any situation.

Additionally, management may be interested in learning how to profit from security offerings. These guides and tools help define the opportunity and detail important things to know before getting into a new security service offering.

- **IT Security Assessment Wizard:** CompTIA's IT Security Assessment Wizard is a straightforward, three-page questionnaire intended to help build a profile of the interaction between your business and one of your clients.
- **Quick Start Guide to Physical Security:** The demand for physical security is changing and providing opportunity and profit for many organizations. Learn some practices to prepare your company for this evolution.

Insist that your full staff, privileged users, security-specific personnel, management, and executives have the proper understanding of their role in preserving a secure environment. Their understanding will support the security control processes required to function as an IT organization.

2 Processes

Think of data security as a system, akin to your own circulatory system. Inside you is a network of arteries, veins, capillaries, blood cells, and organs working in concert to keep you whole body functioning properly. When you need an increase in oxygen, your body detects and responds accordingly. If something goes wrong, a collapsed artery or blockage, warning signs are transmitted and without intervention, the entire system can breakdown.

Cybersecurity works the same way. A system of identification, protection, detection, response, and recovery working in concert to keep your organization healthy. And just like health experts provide guidance on how to maintain and optimize your circulatory system, IT security experts have devoted countless hours crafting guidance for cybersecurity systems.

The National Institute of Standards and Technology (NIST) publishes a Cybersecurity Framework designed to do just that. And CompTIA has applied that framework to the specific needs of IT organizations in the form of the **CompTIA Channel Standard for Cybersecurity**. Furthermore, that framework has been paired with an assessment process to demonstrate how well an organization has implemented those best practices in the form of the **CompTIA Security Trustmark+**.

This section addresses the fundamentals of those standards and provides the resources to help you implement the recommended best practices therein.

STANDARDS AND FRAMEWORKS

By maintaining the perspective of cybersecurity being a system that functions in concert with the rest of your business, you can begin to see the value of relying on best practices for that system. Additionally, compliance regulations become a little easier to comprehend and achieve.

The trap many businesses fall into when it comes to compliance audits is the idea that there must be a rush of work and updates and communications in order to pass the audit during the time the auditors are there. Instead, an audit should be a time to let your well-oiled system shine. Using the comparison to our circulatory system again, it would do you no good to go on a crash diet and exercise program in the 3 weeks leading up to a visit to your doctor. Your overall health and well-being are better suited by implementing best practices for your health every day. Security is the same thing.

Within the Framework, NIST has categorized the "5 Pillars of Security". These pillars are also reflected in the CompTIA Channel Standard for Cybersecurity. Daily action in these 5 pillars is a great way to fine tune your cybersecurity system and demonstrate regulatory compliance, if applicable.

1. Identify: Take stock of assets. Define the environment in which the business operates. Document governing procedures. Understand the risks and tolerance levels.
2. Protect: Mechanisms for access control, awareness and training, securing data and information processing, on-going maintenance, and protective technologies.
3. Detect: Recognize anomalies and events, continuous monitoring, and processes for detection.
4. Respond: Be able to analyze events, communicate effectively, make improvements, mitigate events, and plan for response.
5. Recovery: Plan for recovery, make improvements, and communicate appropriately.

Help in implementation is available. These FREE resources are available to everyone, because it is in everyone's best interest to adopt the recommendations to the best of their ability.

- **NIST Cybersecurity Framework:** Created through collaboration between industry and government, the Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.
- **CompTIA Channel Standard for Cybersecurity:** Based on the NIST Cybersecurity Framework, this Channel Standard is designed for IT organizations and their unique role as handlers of data.
- **NIST-HIPAA crosswalk:** A reference of how the NIST Framework underlays HIPAA regulations.
- **SANS Institute Policy Project:** The ultimate goal of the project is to offer everything you need for rapid development and implementation of information security policies. You'll find a great set of resources including policy templates for twenty-seven important security requirements.
- **CompTIA Security Trustmark+:** For a small fee, CompTIA Members can pursue the CompTIA Security Trustmark+ as a means of validating their cybersecurity system, policies, and processes.

We've addressed the people and process portions of a cybersecurity system. You can see how those are mutually dependent on one another; guidelines implemented by trained staff who in turn make real-life recommendations back to the guidelines for improvement, which leads to staff better equipped to address events. Next we turn to technology and the tools people will use to execute the process.

3 Technology

Our industry moves too fast for this toolkit to provide a run-down of all the great technology solutions available to help you achieve your security goals. And as a vendor-neutral non-profit association, it would be out of character for CompTIA to recommend one product over another. Instead, this section will provide ways to stay in touch with industry and new technology solutions available.

WHAT TECHNOLOGY IS RIGHT FOR ME?

Acquiring the right tools to support your people and processes can mean the difference between daily frustration and operational efficiency. You probably get this question regularly from your own customers, and you should listen to your own advice!

1. Build your requirements – there are two sides to this coin.

a. Determine the business outcomes you desire. Just as you would press your customer for more information, press yourself. This is more than thinking, "I need a firewall." Consider what the business can do (or couldn't do without it) with a solution in place. It has to fit into the overall system.

b. Ensure the functionality meets your requirements. This is where a lot of people like to jump straight into. But if you don't first consider the desired outcomes, you'll be stuck comparing checklists of features. It's important for the solution to have the features you need, but only if the solution first satisfies the outcome.

2. Find the right provider and solution

a. As an IT service and solution provider, you are familiar with the fact that many customers have already done most of their research by the time they talk to you. This is your chance to turn the table a bit. Here are a few tips on finding a tech partner.

i. Industry Events – Attend them. Scour the vendor exhibition. Know what you want (point 1 above) before you get there.

ii. Referrals – Your personal and professional network are vital. Get honest experience from someone you trust.

iii. Member Communities – Peer groups, purchasing groups, vendor partner communities, professional societies, and trade associations all offer great opportunities to meet quality people with amazing solutions from across the industry.

iv. Internet Research – This is the golden age of information availability. Content marketing and white papers are good ways to get a deeper dive into an issue and solution. Reviews, alternatives, questions to ask…there is a plethora of information at your fingertips.

3. Manage the implementation and organizational changes

a. You know you've seen how poorly a solution will perform if the staff rejects it. And you know what you would suggest to your customer if they struggle with this. Again, it's time to follow your own advice.

i. Prepare staff for coming change by getting their input during the requirements definition.

ii. Keep staff abreast of the purpose of the solution and how it will assist them in their duties.

iii. Train users on the new technology solution.

iv. Have a support system in place to help with early adoption hiccups.

v. Reinforce usage with recognition or other perks and reminders to encourage full adoption.

WHAT ABOUT PARTNERING?

Sometimes, the best option is to not just purchase a bit of tech to facilitate security operations. It may be in your best interest to foster a partnership with another business that has more experience, expertise, or a unique solution that really fits your needs. CompTIA can again help you there with both education and our Member Communities.

- **IT Security Community:** Our IT Security community watches the security landscape to help you stay on top of the ever changing challenges and opportunities in IT security. Our mission is to help you protect your clients business as well as drive profitability and growth in your own.
- **Quick Start Guide to Profitable Partnering:** Learn the six strategies every business needs to discover the right channel partners and to use the sales channel most effectively. How can the 80/20 rule work for you?
  - **Quick Start Session to Profitable Partnering:** This recorded presentation of the above Quick Start Guide can help you make your partnerships a more profitable investment of your time and resources.
- **Executive Certificate in Profitable Partnerships with your Vendors:** This intensive four-course program leads you to a mastery of establishing and managing partnerships in the sales channel. See the big picture and set the right course.

So far, this toolkit has covered the 3 legs of the stool upon which your cybersecurity system sits. By selecting and training the right people, supporting them with the right processes, and implementing technology solutions designed to achieve the purpose of the process, you can have a robust and effective cybersecurity system in place.

All 3 of these topics are applied daily. But sometimes it's useful to take a step back from the daily grind to imagine what can come next. To help you there, CompTIA provides amazing research studies and briefs.

4 Research

CompTIA Research and Market Intelligence provides timely, relevant data and insights aimed at informing and driving the IT industry. CompTIA has a library of over 100 research reports, whitepapers, videos and webinars, with new material produced each month. Using rigorous research techniques, CompTIA collects data from tens of thousands of end users and IT companies on a wide range of issues covering tech trends, channel dynamics and the IT workforce.

Being aware of trends and new technologies is a great way to stay on top of things. No one is expecting you to read research briefs every day, but when a strategic decision has to be made about what should be next for your firm, or if you do have to recover from an event and you're looking for ways to improve, CompTIA Research should be on your list of information to review.

Here are some recent studies in the realm of cybersecurity. But the latest are always found **here**.

- **Trends in Information Security:** This study provides insights into the behaviors, techniques and opportunities with IT security as businesses use new technology.
- **Practices of Security Professionals:** This study examines the security usage and practices of IT security professionals, as well as workforce perspectives.
- **Security in the IT Channel:** Examines the practices of channel firms focused on security as a primary line of business.
- **International Trends in Cyber Security:** Discover when and how 1500 IT security professionals outside the U.S. are changing their approaches to cybersecurity.
- **The Evolution of Security Skills:** This study examines the state of security skills in business—which skills are needed, which business units need training, and what companies are doing about the problem.

Research is available through many other outlets beyond CompTIA. But as a Premier Member, there is no better place to get your hands on this information at no additional cost to you.

5 Conclusion

From a practical standpoint, IT security comes down to some basic things. You may not be able to prevent everything coming your way, but by implementing the suggestions found in this toolkit, you can have a puncher's chance.

- **Prepare your people:** training on how to recognize phishing and social engineering, clear guidelines to follow, and opportunities to learn more.
- **Embrace a process standard:** the fundamentals of IT security are defined by multiple organizations. Stand on those shoulders and adopt industry-recognized best practices for data security.
- **Supplement with technology:** IT solutions grow more adaptive and predictive every day. Find a solution that fits your needs and keeps your network secure.
- **Keep an eye on the future:** new threats are just around the corner. Due diligence is your best defense.

CompTIA Worldwide Headquarters
CompTIA Certifications, LLC
3500 Lacey Road, Suite 100
Downers Grove, Illinois 60515

630.678.8300

CompTIA.org