Technical Support
INTERNATIONAL
Consulting and Computer Services

CYBER SECURITY POLICY STARTER KIT:

10 Critical Policies that Every Company Should Have in Place

Today's cyber security climate is more volatile than ever and the volume of potential threats your organization will be exposed to is only going to increase as time goes on.

Unfortunately, "volume" isn't the only thing you have to worry about when it comes to cyber-attacks. Yes, they're becoming more frequent, but they're also becoming more sophisticated, too. Long gone are the days where your only worry was with the occasional, simple virus whereas today, hackers are using increasingly sophisticated intrusion methods- like phishing- that are as authentic-looking as they are potentially devastating.

Because of that, it is imperative for all organizations to begin the immediate and rapid shift of their company cultures and the ways they approach cyber security. It's not enough to simply acknowledge that cyber security is important, you now -more than ever- need to have plans and procedures in place to proactively combat and ultimately mitigate their impact. This, of course begins at the policy level and is reinforced with the complete support of your company's leadership team behind it.

Due to today's increased exposures to cyber-risk as well as compliance driven IT requirements, IT can no longer be siloed to one department or individual IT manager. A truly effective cyber security strategy requires an "all hands on deck" approach and assigning real responsibility to the executive level is going to be essential for keeping up to date with IT security, compliance requirements and your own evolving IT policies. To that end, the most critical thing for you to remember is that a chain is only as strong as its weakest link; If your cyber security policy has a weak link, you're assuming a far bigger risk than you may have previously assumed. For far too long, too many organizations have looked at IT as a separate entity, as something relegated to the "kid's table" at a family dinner when it's now clearly the time for IT to take their seat at the "big person's table." As cyber threats evolve and grow, so must your IT security policies.

What follows is pulled directly from our toolbox here at TSI and has been modified to use as a starting point for creating the cyber security policies for your business. Keep in mind that when you sit down to write your own policies from this foundation, while you can certainly use this as inspiration, every company is unique and you might not need everything that we provide here. Conversely, you might need to add additional policies that we haven't included below. In any event, this should give you a good place to start to begin formulating your own which will hopefully encourage company-wide dialogue and collaboration. By understanding as much as you can about what these policies are, what they're designed to do and why they are so important, you'll be well on your way to creating an effective set of cyber-security policies for your organization and hopefully mitigate the impacts of any potential issues within your network. With that, here are the critical policies that absolutely every company should have in place to ensure their continuity within today's hostile IT landscape.

CHRIS SOUZA - CEO, TSI

Chris brings more than two decades of experience empowering businesses to use their technology in a way that gives a true competitive advantage.

Eager to connect with other business leaders, Chris can be reached through the TSI website or on LinkedIn.

What is a Cyber Security Policy?

A policy is defined as a course or principle of action that is adopted or proposed by a business (in this case), yours. In other words, it's something that the people in your business follow in an effort to prevent or minimize the chances of something bad from happening, to address compliance requirements and/or to easily isolate points of failure for seamless recovery and remediation. Cyber security policies, as their name indicate, are ones designed to keep your confidential information secure and network infrastructure and data as safe as possible.

When creating your own policies, be as specific as possible. Use the "overview" to generally outline what your policy is, use the "purpose" section to break down the reason why a policy is so important and what it's designed to prevent and finally use the "scope" section to detail who in your organization is affected by this policy, then, of course, detail the policy itself.

1

COMMUNICATIONS POLICY

1.1 Overview:

Business communications have drastically changed in the recent past, making us more efficient, productive and informed than ever before. To ensure that these communication platforms – such as social media, text messaging, email and phone- are used as an advantage rather than a vulnerability, it's important to have a firm communications policy in place. One such powerful communication tool- email- is the most used form of communication in nearly every type of business as well as one of the more prevalent way hackers infiltrate networks. End user misuse of email- or of any communications platform- can not only pose both privacy and security risks, but can expose an organization to costly legal and non-compliance issues as well.

1.2 Purpose:

Your Communications Policy needs to cover what is considered appropriate for any communications exchanged between your employees, clients, vendors and any other agents operating on behalf of your company. In conjunction with the security tools that are part of reinforcing a sound communications security policy, a considerable amount of continuous end user training is required as well, especially in regard to combatting phishing and any other techniques hackers may regularly employ.

1.3 Scope:

This policy should apply to your entire company, as well as clients or vendors and be routinely reviewed and discussed.

1.4 What to Include:

This policy should include directives on how any and all communications platforms are used as well and managed moving forward. Things like email for example, should be retained only if it qualifies as a viable business record and all data contained within it needs to be secured according to the Data Protection Standard at all times.

2

PASSWORD COMPLEXITY GUIDELINES

2.1 Overview:

Passwords are often a user's first line of defense against allowing their sensitive information from falling into the wrong hands. Oftentimes, poorly constructed passwords leave users unnecessarily exposed to cyber threats, therefore, complexity requirements – along with the frequency of password changes – become of paramount importance.

2.2 Purpose:

Password Complexity Guidelines should be developed to provide a set of best practices for creating strong passwords across the different organizational levels. This policy provides additional information about how often passwords should be changed, how passwords should be stored, and their mandated degree of complexity in order to maintain the highest degree of protection. For an additional degree of protection for employees accessing your organization's most sensitive data, implementing a fine-grain password policy should also be included.

2.3 Scope:

This policy should apply to your entire company.

2.4 What to Include:

The policy should include examples and rules governing what constitutes a strong password (meaning the use of numbers, symbols, other special characters, etc.) in addition to examples of weak and insecure passwords that should not be used under any circumstances. Any exception to these password construction guidelines needs to be approved by an IT manager, and that team should have the ability to force users to change their passwords in accordance with best practices within 30, 60 or 90 day intervals.

This policy should also discuss how passwords should be stored and categorized based upon their criticality; The higher the criticality, the fewer the people who should have access to those credentials. There should also be verbiage around what groups of people can access the passwords at each categorization level as well.

Another overlooked, yet seemingly obvious policy rule that should be included is to never share your passwords-even if you feel that you trust this individual or feel the communications platform is secure! Similarly, people need to be careful to not "accidentally share" their password – like by writing it on a Post-It note that is then affixed to their computer monitor. It is not recommended that users employ the "Remember Password" feature of applications like web browsers, and if any password manager solutions are used, they must be approved by an IT manager and organizational management before they are implemented. Although password management tools are designed to address these very issues, and we encourage clients to use them, many password management tools do not adhere to regulatory compliance requirements, have a history of being compromised themselves, and should be evaluated beforehand.

3

WRITTEN INFORMATION SECURITY POLICY (WISP)

3.1 Overview:

A Written Information Security Policy is designed to act as a single document outlining all of an organization's security measures to protect critical and/or sensitive data as well as link all of the detailed policies it refers to.

3.2 Purpose:

This document is designed to spell out all administrative, technical and physical safeguards that are currently being used to protect any sensitive or critical information the company is storing. This is the foundational policy of a Cyber Security Policy.

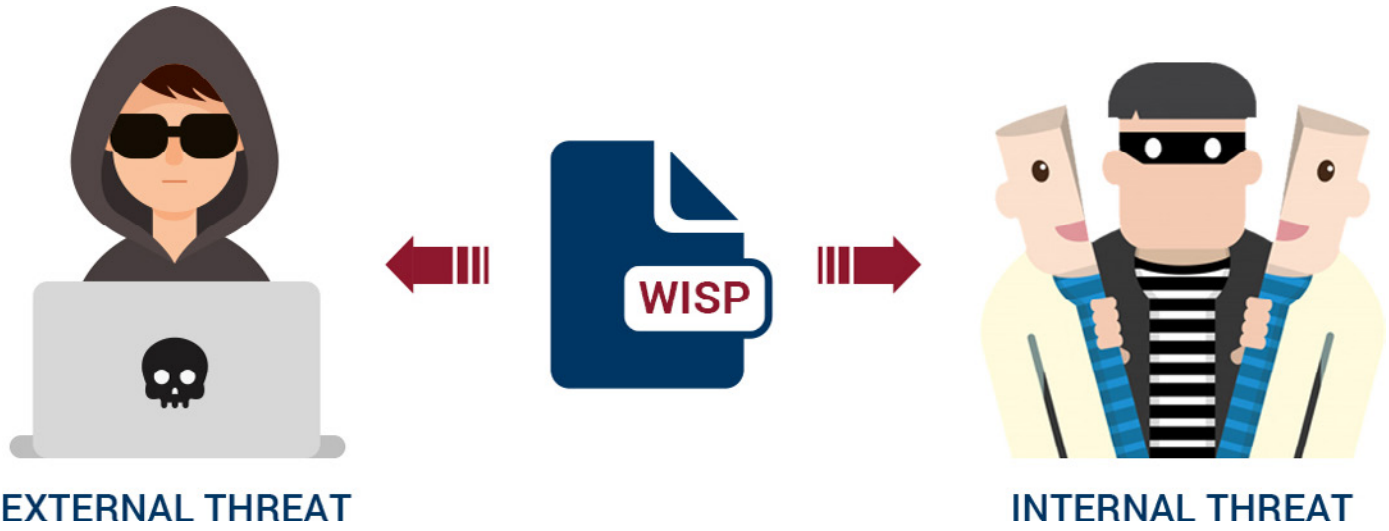
3.3 Scope:

This policy should apply to your entire company.

3.4 What to Include:

One of the most important parts of a WISP is a section that outlines the role of a designated employee- oftentimes a CISO-who will be responsible for not only implementing security protocols, but also training employees on their use, testing security programs and evaluating all of these efforts on a regular basis. Likewise, a WISP should outline both internal and external threats that exist to personal information.

Internal threats are those like records being inappropriately used by employees, while external threats include situations like data breaches. A WISP should also include notification protocols outlining how affected individuals will be informed in the event of a cyber attack, as well as how the situation will be rectified moving forward.



4

REMOTE ACCESS POLICY

4.1 Overview:

Remote access is often a requirement to maintain team productivity, especially for employees who are spread out across multiple geographic locations. As more and more of the workforce moves towards remote work or "tele-work" environments, policies governing how this technology can be used, how information is remotely accessed, how the exchange of communications are managed, as well as ensuring the latest preventative security tools are routinely updated, have become of paramount importance. This is all especially important, as potential damages include more than just the loss of sensitive or confidential company information, but can greatly impact an end user's productivity, the degree of damage or loss of critical internal systems, the reputational damage of their brand's public image, and greatly increases chances of fines or other financial liabilities.

4.2 Purpose:

A Remote Access Policy intends to define all rules and requirements for connecting to and accessing a business' network from any outside host.

4.3 Scope:

This policy should apply to your entire company, especially if there are employees working remotely.

4.4 What to Include:

This policy should outline exactly who can and cannot remotely access your business' network and from what devices. Only employees who need remote access to do their jobs should be granted permission to use it and inventorying all technologies to help identify and in turn protect the valuable information that is being accessed, created, stored and shared. This policy also includes policies for at-rest and in-transit encryption, which remote access programs are to be used as well as the types of Internet connections that can be used.

5 CLEAN DESK POLICY

5.1 Overview:

A Clean Desk Policy is one of the most simple and effective security mandates that can greatly minimize your exposure to a security breach. Not only does it clarify the physical state of one's desk, it also requires that all sensitive and/or confidential information is removed from an end user's working environment. An all too popular examples of a clean desk policy violation would be a user leaving their desk unsupervised while staying logged into their user account, leaving passwords on post-it notes for anyone to see or posting the WiFi credentials for non-guest networks.

5.2 Purpose:

A Clean Desk Policy is important because, while straightforward, it is one of the best ways to reduce the risk of security breaches in the workplace.

5.3 Scope:

This policy should apply to your entire company.

5.4 What to Include:

All computer workstations need to be locked when that workspace is not occupied, or automatically locked after 10 minutes of non-use are one of the fundamental rules included in any Clean Desk Policy. Filing cabinets containing restricted or sensitive materials must be locked and closed when not in use and laptops must either be locked in a drawer or with a locking cable under the same conditions. Users should never leave sticky notes on their desk that include their user or network credential for things like Wifi and use an approvedpassword management solution, instead.

6

ACCEPTABLE USE POLICY

6.1 Overview:

Inappropriate use of computer equipment and other electronic assets is more than just unprofessional; it exposes your entire infrastructure to risks like virus attacks, intrusion attempts, actual system breaches and all of the costly legal issues associated with non-adherence to security best practices. These rules are designed to protect both employees and your organization from digital harm and can also help address one of the biggest hidden costs of any organization: DOWNTIME. The review of your Acceptable Use Policy should be routine and provide another opportunity for companies to evaluate their WISPS, or "written information security policy" with employees.

6.2 Purpose:

Simply put, an Acceptable Use Policy outlines how the various platforms at your company, such as the network, your website or subscribed services, should be used.

Furthermore, it's important to clarify that this is not limited to the previously referred to platforms, but also includes the governance policies over any devices or assets connecting to your network.

It's about maintaining visibility over how your network is accessed, who is accessing, from where and how.

6.3 Scope:

This policy should apply to your entire company.

6.4 What to Include:

All information can only be accessed, used and shared to the extent that is necessary to fulfill an employee's assigned job duties.

7

TECHNOLOGY EQUIPMENT DISPOSAL POLICY

7.1 Overview:

Sensitive company data is often stored on a wide range of mediums, such as hard drives, workstations, and USB sticks. In the event that these resources are being disposed of or otherwise retired from use, they need to be removed and decommissioned in a compliant way to make sure that all of this information is destroyed and unable from falling into the wrong hands.

7.2 Purpose:

This policy defines the guidelines for the proper disposal of technology equipment for all assets owned by your company.

7.3 Scope:

This policy should apply to your entire company.

7.4 What to Include:

Once a specific asset has reached the end of its useful life, it should be sent to an equipment disposal team, or more commonly, an outsourced asset disposition specialist, for proper disposal and to ensure its securely destroyed in accordance with the latest industry or compliance standards and best practices. Remember that true disposal not only requires its complete physical destruction, but a certificate verifying that it's been done by a verifiable asset disposition specialist or ITAD.

8

INCIDENT RESPONSE PLAN POLICY

8.1 Overview:

An Incident Response Plan Policy is exactly what it sounds like; a detailed set of processes, directives and best practices that are to be followed in the event that your organization suffers any intrusion attempt or security-based incident. For some compliance requirements, it mandates that ANY security issue - whether it's a simple virus or complete breach - to be easily identified, isolated and reported upon; Again, this is not just limited to "significant" issues. In addition to this, many regulatory requirements also mandate that you're able to readily understand when the breach occurred, how it happened and what needs to be done to recover from the incident. Unlike the the other security policies outlined within this article, this policy goes into effect once a data breach has already happened and is no longer a hypothetical. At this point, you're no longer trying to prevent any given problem from happening, you're trying to mitigate the damage as much as possible moving forward, in accordance to the established policy in place.

8.2 Purpose:

Incident Response Plan Policy is another policy designed to help teams create a greater sense of awareness and communication in times of crisis, all the while giving them a chance to coordinate their efforts for the most effective response possible. It's encouraged that this plan is regularly reviewed as part of a routine "fire drill" style exercises within your company, as well.

8.3 Scope:

This policy should apply to your entire company.

8.4 What to Include:

The key to this policy is specificity. Not only should all business units supported by your information security team or MSP develop and maintain a security response plan, but the plan also needs to be designed in a way that allows for the easy sharing of all information required to formulate a successful response in the event that a particular type of security incident occurs.

This policy needs to include a specific set of instructions that are to be followed by all relevant parties in the event of a data breach, including the break-down of the specific types of breaches that could occur. A breach that occurred as the result of a phishing attempt would require a totally different response from that of a larger and longer lasting network intrusion such as Ransomware. Not only would a solution to the problem require a totally different plan, it's likely the extent of the damage will be far different as well in that different information will have been accessed and compromised. Because of that, you need unique plans for every possible scenario so that people can quickly and effectively respond in the event that anything happens.

This policy should also include verbiage about who should be notified (vendors, customers, law enforcement, etc.) based on the type of data that was breached and the timeframes in which these parties should be notified. Keep in mind that certain types of data are regulated and have mandatory notification timeframes.

But more than anything, how cyber incidents are handled across an enterprise reflects a foundational principal of establishing a culture of openness, trust as well as integrity amongst employees but those of regulatory agencies, vendors and clients too. If a theft, breach or exposure ever occurs, this policy will lay out specific steps involved to remediate as well as help mitigate the issues stemming from the incident. This is also a part of the majority of regulatory compliance requirements your organization is likely to deal with like DFARS, ISO 27001, CMR17 or HIPAA.

9 DISASTER RECOVERY PLAN POLICY

9.1 Overview:

One of the most unfortunate gaps in the security mindset of a lot of organizations is their incomplete understanding of their disaster recovery capabilities in the event that a disaster occurs. Because complete infrastructural disasters happen so infrequently, management often overlooks the recovery planning process and what it entails entirely. Even worse, these plans are usually not updated as often as they should be, causing them to grow ineffective over time as both the factors and nature of the issue contributing to disaster frequently change. This idea of routine policy review is at the core of a Disaster Recovery Plan Policy, which encourages businesses to take a closer look at any event that could likely cause "an extended delay of service" as well as the potential operational and financial impacts the issue presents to their organization.

9.2 Purpose:

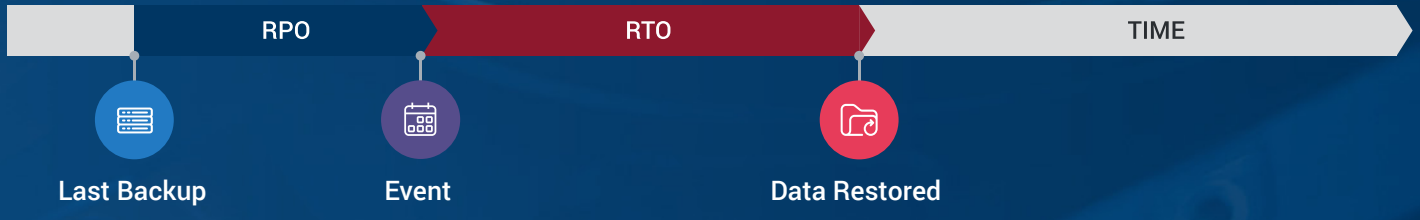
Your Disaster Recovery Plan should be designed to not only provide a series of detailed steps that people can follow to quickly recover from any given type of disruptive event but should also detail the different procedures for specific kinds of events that may occur. One might outline the available contingencies stemming from a major "act of God", while another might outline the steps for recovering from a major, company-wide disaster like Ransomware.

9.3 Scope:

This policy should apply to your entire company.

9.4 What to Include:

Disaster recovery plans are not isolated to simply implementing a robust backup solution but extend to the processes required to recover from a disaster and can include the steps required to relocate your business all-together. These plans should be kept up-to-date in an effort to mitigate the risk from these types of events moving forward and should be tested at least quarterly- if not more frequently. Not only does this ensure that your policies remain effective given any changes to your infrastructure, but it also enables you to implement policies to address newer threats. You should also be aware of your company's RTOs (recovery time objectives) and RPOs (recovery point objectives) when formulating your policies and implementing a backup solution complimenting those objectives. Where RPO speaks to your degree of tolerance in regard to the quantity of data you can lose, the latter speaks to the amount of time that can pass before your business begins to experience unacceptable consequences.



10
BYOD POLICY

10.1 Overview:

As consumer technology becomes more prevalent in the workplace as an acceptable business tool, it's critical to ensure that any BYOD (Bring your own device) environments are adequately secured to minimize the chances of a breach or degree of vulnerability of critical organizational data. If employees are accessing email through their phones or personal tablets, it's absolutely critical that a policy exist either restricting the use of these devices or that it outlines the system requirements for BYOD users such as maintaining updated anti-virus and/ or requiring management agents on those devices.

10.2 Purpose:

Your BYOD policy, should clearly outline the system requirements for those devices- if they're allowed- including any other precautions to ensure those devices are not presenting a security issue to your environment.

10.3 Scope:

This policy should apply to your entire company.

10.4 What to Include:

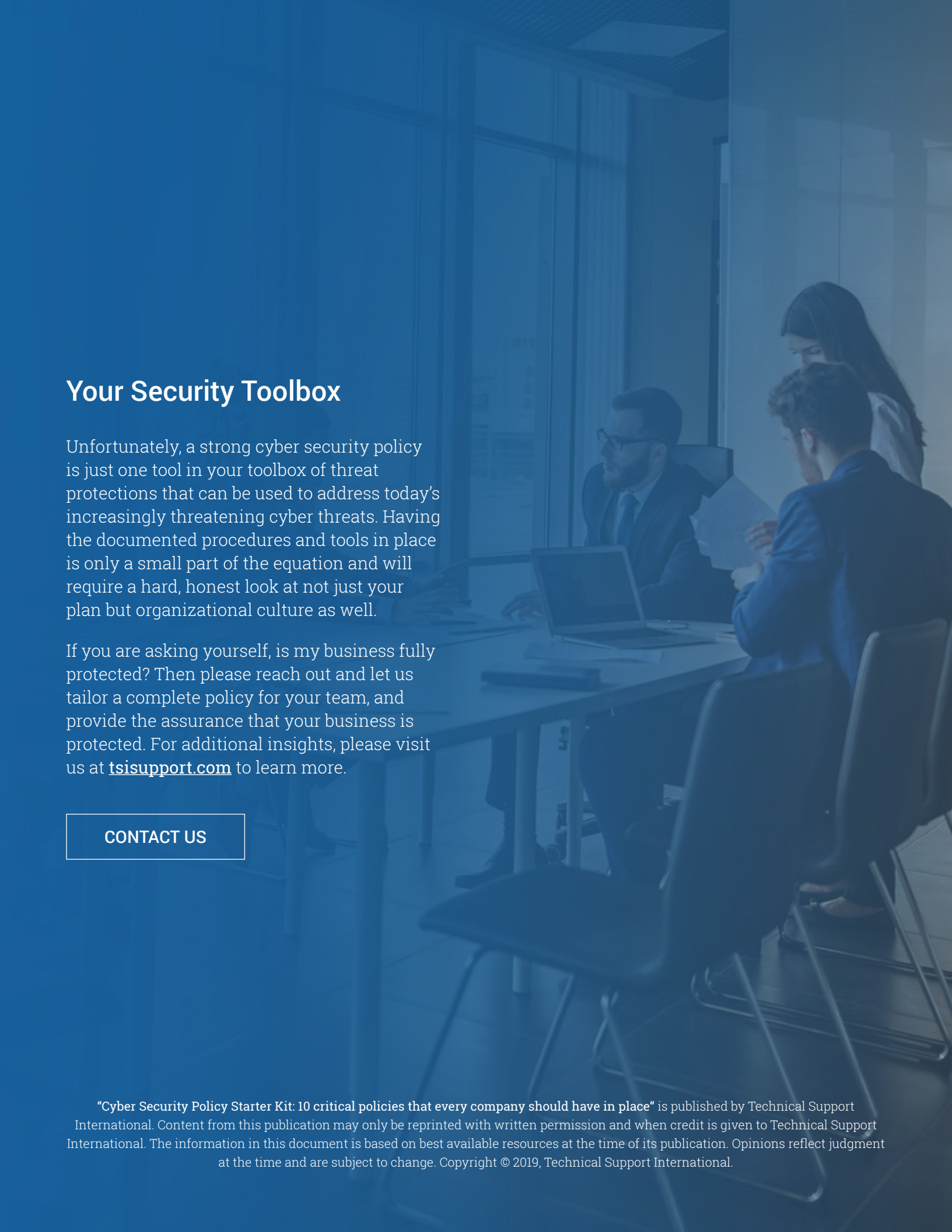
The policy should be very clear and, similar to the Acceptable Use Policy, should outline what is considered the acceptable use of employee devices, the type of information exchanged, list of approved company applications, as well as the steps required to vigilantly maintain device security. Because BYOD is a common reality for many organizations, it's typically found in employee handbooks as well and regularly reviewed and updated to address any changes to the cyber security landscape.

In the End

Overall, it is critical for you to understand that an effective cyber security policy is a "living document" that routinely incorporates changes addressing the dynamisms of today's cyber threats, verifies the effectiveness of your policy and ultimately the strength of your security posture; This is not a "once and done" type of exercise.

Security is also about proactively minimizing your chances of becoming a target. The chances are high that at some point -if not already- that you will attract the attention of hackers, and by having these policies in place and enforced, is a significant step to lowering those chances. If anything, not only will these types of security tools and controls minimize the impact of a security incident, they will at the very least, show that you have done everything you can to defend against these types of situations which is often more than worth the effort- especially when you're presented with a considerable penalty for non-compliance!

All in all, organization-wide cooperation - starting with leadership on down - is required to truly maintain the strongest security posture possible today. Assigning these responsibilities to only your IT department, or "siloing" off your efforts into a series of disparate parts that do not communicate or collaborate with one another, is more so than often, a recipe for disaster.



Your Security Toolbox

Unfortunately, a strong cyber security policy is just one tool in your toolbox of threat protections that can be used to address today's increasingly threatening cyber threats. Having the documented procedures and tools in place is only a small part of the equation and will require a hard, honest look at not just your plan but organizational culture as well.

If you are asking yourself, is my business fully protected? Then please reach out and let us tailor a complete policy for your team, and provide the assurance that your business is protected. For additional insights, please visit us at tsisupport.com to learn more.

CONTACT US