Cybersecurity Assessment Questionnaire 10 (+1) Best Practice Preview 2020 Edition

This sample of our comprehensive service provider sales enablement tool covers some of the key questions and best-practice answers needed to assess your prospects' and clients' cybersecurity posture.

Service providers and IT professionals need to help organizations understand their cybersecurity posture and their level of vulnerability and risk. Full Security audit projects are costly, time consuming, often use out-of-date tools and concepts. Yet some fundamental truths remain. That's where the NIST Cybersecurity Framework comes in. First published in the USA by the National Institute of Standards and Technology in 2014, the NIST framework can help an organization build or strengthen their cybersecurity program. Since it is a standard that is well understood by everyone from experts to generalists, it can be used to start conversations about cybersecurity and risk management across an organization.

To facilitate your ability to make a security assessment of potential clients during the sales process, or an assessment of existing clients, we have created a security assessment questionnaire. The questions are worded in simple language and are organized and coded according to the categories of the NIST framework: Identify, Protect, Detect, Respond and Recover. The related NIST Function and Category Codes follow each question, and a code key is available at the end of this document. We believe these questions and the findings you will uncover will provide your team with insight into the organizations' cybersecurity program and posture.

Acronis

WE HAVE CREATED THE FOLLOWING TOOLS:

1. Full Assessment Questionnaire
2. Full Assessment Questionnaire with Answers (2020 edition)

Here are the best practices for each of these:

- **Download** the Assessment Questionnaire Microsoft Word document. Customize it by removing and adding questions that are aligned with your services. This document is for your organization to brand and use as a tool to perform security assessments.
- **Review** the Assessment Questionnaire with Answers **(2020 edition) PDF document.** A cybersecurity professional has reviewed the Assessment Questionnaire and provided simple-to-understand background and answers on why the assessment question is important — and, in many cases, a related tip.

PROCESS

Download the Full Assessment Questionnaire doc, customize the questions and document as you require. This is a brandable and document your team can use as a sales enablement tool.

Review the Full Questions and Answers.

Build an assessment plan and suite of tools that your teams will use to capture the answers for the questions. In many cases, an interview with an IT Professional or simple reviews of endpoints will provide the needed insights.

We hope that your team finds the Assessment Questionnaire and Answers valuable and that your clients will have a stronger security posture after you've identified gaps, planned improvements and implemented them. Feedback is always welcome and we'd like to hear from you on how this assessment and questionnaire could be made better for future updates.

IDENTIFY

Do you have visibility of all connected users, devices, data and services across your network?
[ID.AM]

If you don't know that something is happening, you can't do anything about it. That's why network visibility is a key component of NIST's Identity and Access Management.

With increased visibility, you can better protect your network from problematic devices, users and services. This is because you have a much better chance of intervening if something unusual, dangerous or unexpected happens.

With the right tools and services, you can see and interpret everything that takes place on your network.

For example, you can monitor network activity, see what devices have connected, who owns which device, what services are accessed by whom and when.

There is a wealth of useful information available that can better protect the network, its users and your business partners and customers. But a note of caution: if an administrator is presented with too much information, illogically organized, it can lead to security oversights.

Choosing visibility tools that simplify monitoring activities taking place on the network is the name of the game. The services and available configurations should underpin your business and security requirements.

TIP

Ensure your access management tools provide easy-to-digest log information for stakeholders that highlight any important issues. These can simplify information security authorization requests.

Quality management software, such as Acronis Cyber Protect, offers a single solution to integrate remote desktop, backup, disaster recovery, AI-based protection against malware and ransomware, and security tools in a single agent.

Simple detection and onboarding of new devices needing management and protection reduces both workload and potential exposure.

PROTECT

Can you remotely access, configure, audit, track and securely wipe any devices you allow on your network, even when they are outside of your network?

[PR.AC]

Being able to manage remote workers' accounts, devices and access rights at the touch of a few buttons is an incredible advantage, particularly when, in 2020, we are facing so many people having to work from home for the first time.

Device management refers to software that is used to oversee, regulate, and secure employees' portable devices. It can include a host of services, including user, application, service, access and content management.

Users may try to access the network with unauthorized devices or accounts; they may have configuration issues; their devices may be compromised. Issues like these are easily resolved with a reputable remote tool that simplifies the daily management of remote devices, whether they belong to the company, the user or a third party.

TIP

Integrated security solutions, like Acronis Cyber Protect, can offer Remote Desktop access as a built-in feature, so you don't need to use different consoles and systems to manage your security requirements, and manage users working offsite.

Do you track all systems, services, users, and contact lists to ensure anything unwanted or expired is deactivated or disabled?

[PR.AC and PR.DS]

Accidentally sending unauthorized users sensitive information can lead to a whole world of trouble. Not only can it be embarrassing and likely to have a reputational impact, in some cases, you will even need to notify the authorities, especially if user account information was shared inappropriately.

Regularly reviewing the network to see what systems, services, and users are currently authorized is highly recommended.

A key question is this: Do any need to be removed? Added? Edited?

This is often referred to as 'tidying house' This approach verifies that the right information is accessed by the right people at any given time, and that old, unwanted or expired information is removed.

Information management is simplified if you have intimate knowledge of your system and services. Regular maintenance of accounts, systems and services can radically reduce the complexity of a network. These reviews, done regularly, can reduce your threat exposure dramatically.

TIP

Integrated management software like Acronis Cyber Protect can radically simplify tracking your systems and onboarding new ones, ensuring all required security and backup protections are in place as soon as a new device is detected.

Are all users given regular cybersecurity awareness information and training, covering how to avoid the latest threats (eg malvertising, cryptomining, phishing, social engineering, and ransomware techniques)? [PR.AT]	Most security incidents take advantage of a user's lack of information security knowledge. Having a cyber-smart user base is a strong line of defense, underpinning your security services. Most of us who work in information security know that the online world is rife with phishing attacks, malvertising and other scams, often employing social engineering tactics — all designed to dupe the user. With a little education, users can change how they interact with the internet, making them safer online, both as an employee and an individual. Explaining how social engineering tactics work, and why they are successful — using examples where possible — is key. Many users do not understand or believe how they could ever fall into a trap, so teaching them why they and the information or access rights they possess must be properly guarded will go a long way to safeguard your network environment.

TIP

A good tip is to talk to users about improving personal security, using ID theft as a case study. Then you can show how these security lessons can apply to safeguarding the organization.

Cyber awareness training should be provided regularly (at least yearly) to inform users what the latest threats — and the latest tactics — are, so they can help safeguard your environment. Along with a strong security policy, cyber protection training can go a long way to defending the network, and the organization from headaches.

Do you encrypt all sensitive data? [PR.DS]	Encryption can help protect data you send, receive, and store, using any device (a networked computer, or a remote device). It is a key security initiative that every company — large or small — should take advantage of as much as possible. It helps provide data security for sensitive information. Encryption plays an essential role in keeping data private. Encryption effectively scrambles readable text, so it can only be read by the person who has the decryption key. A vast amount of sensitive information is managed online and stored in the cloud or on servers with an ongoing connection to the internet.

TIP

Not only does encryption help to protect your data from unauthorized access, it is also a regular requirement by governing bodies (eg, Health Insurance Portability and Accountability Act (HIPAA) General Data Protection Regulation (GDPR NIS Directive, Telecom Framework Directive and even eIDAS regulations.

Do you have good quality malware protection installed, active and updated on all devices that access your network?
[PR.PT]

Malware can sneak into your systems and networks via all sorts of unexpected vectors. Having protection in place at all different levels minimizes the risk of something nasty slipping through the net.

Selection of a high-quality set of detection and protection tools is just the first step — it's just as important to ensure everything is properly set up and configured to meet your organization's requirements, and that it remains active and updated at all times.

This is another area where central management is a must, not just to give visibility over which systems have which protections in place, but also to simplify the tasks of applying updates and patches, and rolling out changes to policies as your business needs evolve and new types of threat emerge.

TIP

Best-of-breed providers like Acronis Cyber Protect include on-access and on-demand malware detection both locally and in the cloud. With the added benefit of its behavioral engine, you can quarantine events based on suspicious, unexpected or unwanted behavior. Plus, Acronis further simplifies management by combining visibility and control of malware protections with other related features, such as backups and patch management, all accessed from the same user interface.

Are you regularly scanning all the data on your network, including backups and archives, to ensure it is not harboring malware and has not been tampered with?
[PR.PT and PR.DS]

Malware detection can be a multi-stage process. While we rightly expect top-quality anti-malware to spot and block all unwanted items immediately on arrival, some things may eventually slip through this first line of defences. When new threats emerge and have not yet been flagged up by security watchers, and especially where such threats have a delayed or event-triggered payload so no suspicious actions are spotted at first, there's a chance they may find their way into your file systems and data storage.

To make sure anything like this doesn't lurk around long enough to cause problems, regular scanning is a must, and this should include not only data that is in regular use, but also data being archived, as well as the content of backups themselves.

TIP

It's also wise to regularly check the integrity of your backups to make sure there haven't been any unwanted changes which might impact the viability of the backup when you need to restore from it. Leading providers like Acronis Cyber Protect which integrate backup and malware-detection functions can make this process simple and efficient.

DETECT

Do you regularly review the output from your security systems — anti-malware, firewall, IDS, traffic filters, etc. — to spot unwanted behaviours or activity on the network?

[DE.CM]

While we become ever more reliant on systems to alert us to any security problems, we can also get complacent at reviewing alerts, especially if there are a lot of false positives, or if the system security level is incorrectly set.

Those responsible are inundated with alerts, so much so that they stop responding. This is a typical scenario that happens a lot, and it is very important to ensure this doesn't happen in your organization: make sure the security output is properly collected and reviewed, so that automated alerts are responded to appropriately.

Not only does this allow an individual to spot oddities that alerting systems might have missed, but it also helps to ensure that those responsible for the security system have a clear understanding of how each component works (both independently and as part of the network security family), why the services are configured as they are, what information they collect and whether there are any holes that can be proactively closed before they are taken advantage of.

TIP

It can help a lot if your main security monitoring tasks are combined in a single central management system, like Acronis Cyber Protect.

RESPOND

Do you regularly test your incident response plan to ensure that it's not only up-to-date and effective at mitigating dangers, but that it is also easily understood and actioned by all parties?

[RS.AN, RS.IM and RS.MI]

Testing is a vital part of any response plan. It's no use drafting a hugely detailed, comprehensive plan only to discover that there's a fatal flaw somewhere along the way just when you most need the plan to work — in the middle of an incident. Once you've laid out the plan, and agreed on all the required steps with everyone involved, you need to test it out to make sure it works in practice.

Testing should involve everyone who has roles to play in the incident response process, including any backup personnel who may be needed if your first-line people are unavailable or overloaded.

It should fully exercise all aspects of the plan from all possible angles, and most importantly it should be run regularly — your systems and teams are rarely static, and small changes can have unexpected impacts. Once a year is a bare minimum (and is required by some regulations, such as PCI DSS) — quarterly or monthly is much better.

TIP

After each round of testing, make sure any issues noticed are rolled back into the plan to keep it up to date, not just making sure that it addresses the latest threats and attack vectors, but that it properly reflects the changing set of people, hardware and software involved, and the changing needs and priorities of your business.

Have you created and maintained a comprehensive incident response plan to help guide your action during an unwanted cybersecurity event?

[RS.RP]

Having an incident response plan to follow is such a fundamental element to ensure a quick and least painful recovery process.

Without a plan, an organization can quickly lose communication with important parties, overlook key security practices, fail to lock down specific channels, etc.

Even if you have all the tools, but you have not set them to work as you need them to when the proverbial hits the fan, then they won't provide nearly as much value to you.

Creating a plan means you have to look at your environment, what your key users require and how they access it. Once you figure out what is important, you can figure out how to mitigate damage if a potential threat is successful. From a power surge to a power cut; from a data leak to a denial-of-service attack; from ransomware to an insider attack, where an employee walks away with your entire customer list.

TIP

What should happen, who should be contacted, what services are vulnerable? Having all this information listed in an easy-to-follow incident response plan can save you tons of recovery headaches, resource requirements and expenditures.

RECOVER

Do you regularly test that you are able to quickly repair or restore any data, devices or services that may have been compromised by a cybersecurity event?

[RC.RP]

Recovering from a cybersecurity event needs to be as fast and painless to minimize the business impact.

Hard-pressed IT staff will already be overloaded with ensuring any potential gaps in security which facilitated the event are closed off safely, and further interruptions in business as usual have to be kept within acceptable limits.

Testing your recovery and restoration processes regularly ensures that, when they are needed for real, everything runs smoothly and quickly. Potential gaps include key personnel: if your lead admin is the only one who fully understands what needs to be done, or has the only login accounts to key restoration systems, are you sure you can quickly get things back to a known-good state if that admin is off sick, or unable to get online?

In ransomware cases where large amounts of data have been encrypted to prevent access, you need to know you have reliable backups safely stored well away from any area which could potentially be impacted by the attack. You want to make sure that all data can be restored to the most recent possible version without risking any re-infection.

If a website or online service has been hijacked, you need to regain control ASAP. If a user's desktop machine has been compromised with malware, a secure wipe and re-imaging of the entire system is preferable to attempting to clean up the malware alone, and if a good, reliable, well-tested system is in place to do this, it could even be quicker than cleanup.

TIP

Regular testing is not just about making sure your systems and processes are actually working — it's also good practice for all staff involved, so that in the panic of a real event they are well-prepared and able to jump into action.

Quality backup management software like Acronis Cyber Protect can radically reduce the overhead of ensuring your backups are reliable and can be rapidly restored with minimal effort, even applying patches and updates to restored systems for extra speed getting users back to work.

FUNCTION AND CATEGORY UNIQUE IDENTIFIERS

FUNCTION UNIQUE IDENTIFIER	FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Put It Into Practice

Get the resources needed to assess the cybersecurity posture of your clients and prospects for free.