Cybersecurity Assessment Questionnaire

This comprehensive tool covers the key questions needed to accurately assess an organization's cybersecurity posture

IDENTIFY		
	Q	**A**
1	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. 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. ***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.***

2	Is your approach to cybersecurity correctly aligned with the needs and objectives of your organization, taking into account regulatory and legal requirements? **ID.DE and ID.GV**	When it comes to cybersecurity, anyone who touts one size fits all is talking nonsense. State laws regarding cybersecurity requirements vary from state to state, just as industry compliance regulations vary depending on your industry sector. It is important to understand the requirements and how they impact your organization. But this alone will not help your business to grow. Today's security is about understanding your organization's objectives and then aligning your security policies and procedures to protect these objectives. For example, let's say your company sells widgets to a customer base. Each of these customers has an account on your network, and these are regularly accessed by managers. And let's add that we know that a key company objective is to grow the customer base. **The security goal should underpin this main business objective:** • protect that customer's data from unauthorized access. (protecting this information is a key requirement for many industry bodies and state regulators, so this business objective aligns nicely); and • ensure authorized access is as frictionless as possible (this security goal is unlikely to be mentioned by any regulatory body, but it is a key organization and security concern: if access is painful and slow, users are motivated to find a work-around, one that might put the entire network at risk). The key to a strong security policy is a deep understanding of the business objectives, as well as understanding the regulatory requirements. ***TIP: Stay on top of changing business needs and regulations by regularly checking in with all relevant personnel to ensure their needs are being met, and updating policies to accommodate new legal or business requirements. Regular (ideally monthly) surveys or all-hands calls can be a good way to monitor satisfaction.***
3	Are you regularly performing risk assessments to measure your threat exposure (including those from your supply chain, users, business partners and customers)? **ID.RA. ID.RM ID.SE**	Risk assessments perform a number of key tasks to reduce an organization's overall exposure to threats. Risk assessments evaluate the security of services, configurations, user policies, hardware implementation, etc. These risk checks ensure that those in charge of the infrastructure are aware of how the system and services are used, and highlight areas for improved security, such as finding vulnerabilities, lax security protocols, or authentication oversights. It is also important to be confident in the security implementations of your supply chain. Business partners that provide products and services to you and your customers should be able to present you with a recent report on their security risk report to help build confidence in the partnership. ***TIP: Regular risk assessment is a proven method to evaluate your threat exposure. Depending on the industry and the amount of sensitive information processed, they should be performed quarterly to yearly.***

4	Are you correctly insured against any damage or loss from cybersecurity incidents, including employee negligence or insider threats? **ID.RM**	Cybersecurity insurance offers businesses financial protection from the effects and consequences of online disasters, be they a bad agent attack, data loss, data theft, ransomware, malvertising, etc. Cybersecurity insurance is a nascent field. New cyber insurance services and providers regularly enter the space, so we now see a bevy of offerings from both unknown and established insurers. As it's new, it is a complex space to navigate. Players are still jockeying for position in what is touted to be a huge market. Select your cyber insurers as you would any other insurer, remembering that the one offering the cheapest rates may not be the one that returns its investment in any meaningful way. By balancing the cost, the service offering, the reputation, and its customer service, you will narrow your choices to a strong shortlist. ***TIP: As it has not been around for long, be very careful not to assume it is a one-size-fits-all market. Insurers offer a variety of cover options, so it's key to get proper advice on which policies are right for you, should a cyber threat be successful.***
5	Is your organization compliant with the industry's and/or region's cybersecurity operational requirements, as appropriate? (e.g. HIPAA, PCI, GDPR) **ID.GV**	State laws regarding cybersecurity requirements vary from state to state, just as compliance regulations are specific to each industry sector (e.g. medical, financial, legal, retail, etc.). While industry standards vary, depending on the industry and its individual requirements, there is overlap between these bodies (e.g. many regulators will require that sensitive and PII information must be stored securely, that backups are kept and regularly updated, and yearly risk assessments are conducted). But there is no one size fits all. A retail organization that processes payments will have different considerations to those organizations providing medical services, and the individual regulatory stipulations take these all into account. It is important to understand which of these bodies impact the organization. Then you can prioritize the requirements and recommendations these regulatory bodies require your business to follow. There are few things to look out for here. First, ensure your information security partner understands your regulatory compliance needs, whether they are tied to industry standards, federal law, or state law. Building an information security infrastructure to protect your organizations' people, services and assets while also meeting all regulatory guidelines can seem daunting at first, but this approach can dramatically reduce the network's operational risk, as well as help you future-proof the organization against tomorrow's threats. You can simplify the work of ensuring compliance with many regulations, particularly those regarding data retention, with a high-quality backup solution like Acronis Cyber Protect, which is designed for even organizations with strict compliance regulations, e.g. GDPR, NIS Directive, Telecom Framework Directive, or eIDAS regulation. ***TIP: By using one trusted integrated solution that includes data compliance reporting, you can eliminate complexity, improve security capabilities and uptime, all while reducing costs.***

PROTECT		
	Q	A
6	Do you centrally manage and monitor all user accounts and login events on your network? **PR.AC**	Being able to centrally manage and monitor all user accounts and login events on your network gives you real-time control of which users are allowed to access what services at which time. For example, you can set your centralized system to alert you whenever an unexpected or unwanted account request is made, allowing you review it before access is granted. Or you might want an easy way to onboard new hires, or indeed retire accounts of leaving employees. Or, say you notice a huge amount of data being unexpectedly downloaded, a reputable centralized system would allow you to review who is accessing what service at any given time, and select appropriate action. And considering today's internet of things, wearables and personal devices, not to mention BYOD policies, being able to quickly see and control any device goes a long way to protecting your digital assets against unauthorized access, vulnerabilities, or lax security protocols. A good centralized management will store all user activities in a single secure location. The word secure is key here, otherwise a centralized management could become a single point of failure. ***TIP: A comprehensive off-boarding policy is just as important as proper onboarding of new employees. When a user leaves the organization, or changes role, there should be a standard set of steps to ensure any unneeded accounts are disabled or deleted quickly and efficiently.***
7	Can you monitor and manage all file permissions on your network to ensure that data sets are only accessed by active and authorized users? **PR.AC**	Access to the right files and folders is a basic requirement for any digital worker, but it is important to make sure that all users can only access those items and areas they need for their work, and no more. Having central oversight of which users have access rights to which files and folders is key to maintaining appropriate privacy and security without impeding day-to-day business. This particularly applies to shared storage areas, where a simple error in assigning rights can grant a user access to large amounts of information they should not be able to see. Getting this right requires careful structuring of both your data and your rights assignment, usually managed through groups of users aligned to roles or departments. There may be cases where multiple groups need access to the same sets of files - to avoid duplication, it's tempting to place these in areas accessible to different groups, but these should be carefully managed to ensure neither group is inadvertently storing group-specific files in shared areas. ***TIP: Routinely review and update your file permissions at the same time you review user groups and rights allocations, to keep things in sync.***

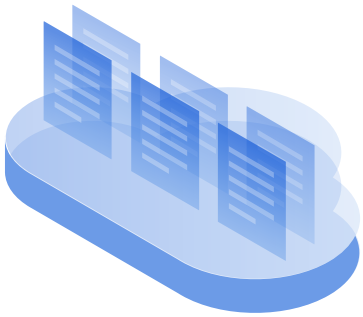
8	Do you prohibit account sharing across all services and users as part of your information security policy? **PR.AC**	Most of us know that account sharing is a big no-no, and yet many organizations continue to operate with shared accounts for a variety of reasons: reduce spend, ease of access, simplification, etc. But it can cripple your chances of spotting and deterring potential threats. **Here are a few security considerations:** • Changing passwords becomes difficult - how would a new password be communicated to all users? • The likelihood of spotting unauthorized users accessing the system becomes difficult, if not impossible. • Once a shared account is compromised, an attack's payload (e.g. encrypting files in the case of ransomware) can spread more widely and quickly. • There is no valid audit trail, and without it, accountability and responsibility become difficult-to-resolve issues. Regularly review your accounts, ensuring that every user is using unique log-in credentials that follow security best practice. Remote desktop access, a feature seen in products like Acronis Cyber Protect, can dramatically reduce the time and resource required to manage users working from home, or anywhere for that matter. ***TIP: To ease the burden on staff and simplify IT's tasks during the onboarding of new users or the removal of old ones, consider employing a reputable, network-wide, centrally managed password management service.***
9	Do you control and monitor what applications your users are allowed to install and use? **PR.AC**	As companies grow, the activities and requirements of their staff inevitably become more complex. The set of applications needed within the network can expand rapidly. This can be exacerbated by staff preferences, when an individual finds the standard tool in use in your environment does not offer the user experience they are used to from previous positions. It's important to restrict users to only known and trusted applications managed and maintained by IT staff, and prevent installation and use of any other tools or solutions. A good rule of thumb is to operate by least privilege: only give users access to what they need for their work, and nothing more. By controlling and limiting what applications each user has access to, you can hinder even a successful attacker's attempts at accessing your sensitive files. Plus, with central management software, not only can you instantly view the login attempts and block a specific user or device, but you can revise access controls to lock down your data and services. ***TIP: Try to make sure all potential user requirements can be met using the set of trusted tools maintained within your system. If a new workflow is scheduled to launch, locate the appropriate software to facilitate it, and set it up, test it, and connect it to your patching and version management processes so it is available when needed. With a little foresight, you can avoid having to urgently add new services at short notice – hurried changes add risk and uncertainty.***

10	Do you enforce best security practices, such as unique complex passwords, multi-factor authentication, and where advisable, single sign—on to users? **PR.AC**	Many companies rely only on a username and password to allow a user to log into a service on the network. The problem with this as a single security measure is that it can also be a single point of failure We know that the majority of successful data breaches begin with an authorized agent getting access to bona fide login information. By using legitimate login information, the attacker tries to effectively hide from detection, sneaking around under the guise of being a legitimate user. Implementing secure authentication policies can greatly reduce your exposure to the risk of hijacked accounts. Multi-factor authentication can be a particularly strong protection against stolen or guessed login details, making a password of limited value to an attacker. Centralized password-management can reduce the overhead of keeping up with large numbers of complex passwords, and helps enforce password strength and account re-use policies. ***TIP: Educate your users on the reasons for imposing secure authentication, so they understand the risk, and the counter-measures they can employ. Combine this with training in how to use any multi-factor or password-management tools, which should emphasise the added ease of use.***
11	Do you have an up—to—date inventory of all third—party applications running on your system, including their patch level? **PR.AC**	The accelerated rate of technological change means that companies today often need to evaluate, install and decommission applications so frequently, it is easy to lose track of the applications running on the system. Every application, if not properly managed, could open the door to unwanted activity on your network. Application inventory is effectively the process of keeping records of all the applications available or installed to a network. Being able to see what applications are installed across your network requires an up-to-date inventory that is both easy to access and understand. In fact, it is rather difficult to imagine how an administrator could perform their day-to-day tasks without having a solid system to monitor all the applications across the network. At-a-glance management interfaces can provide a wealth of real-time information regarding the applications on your network: version number, patch levels, users etc. This is a powerful tool, giving the administrator full control on the applications available. Say for instance an application was found to be vulnerable. An at-a-glance look at your inventory will tell you whether it is installed anywhere, and whether it is patched. That information will allow you to make the decision to suspend its access until it is properly protected, or to implement a workaround to mitigate the danger. ***TIP: There are a number of considerations when choosing inventory tools, including ease of use, reliability, features, customer support, user reviews, and versatility. Make sure to assess the considerations against your specific organizational goals and objectives.***

12	Do you allow IoT devices such as digital assistants, smart white goods etc. to connect to your network? **PR AC**	As more and more hardware devices become "smart" and "connected", the divide between the "computers" managed by the IT team and other devices acquired and owned by other departments - such as catering and facilities - can become blurred. With many IoT device makers paying minimal attention to security issues such as patching and built-in admin passwords, granting such devices access to your key company networks can be risky. If IoT hardware is in use within your environment, there is rarely any need for it to connect to your core systems or networks. To provide internet access to these devices, the best policy is to run a segregated network, keeping all non-IT devices separate from your carefully secured and managed systems. Pay attention also to whether devices require updates or other maintenance from the IT side. ***TIP: Implement a policy requiring IT vetting and approval of all devices connecting to your networks, even low-impact segregated areas.***
13	Do you prevent users from connecting non—authorized devices to your network (physically or wirelessly)? **PR.AC**	If a hacker or another unauthorized user connects to your network, it is important to be able to identify and block this user from accessing any areas that might contain sensitive information. Blocking unknown devices is important, but equally important is having real-time remote management capabilities. A remote access feature, like that found in Acronis Cyber Protect, can radically simplify this task of only allowing known devices onto the network. Here's why: say the boss loses his phone and buys a new one and requires immediate access to the network from their home office, the administrator should have the tools to make these changes quickly and securely (including blocking the old phone and authorizing the new device, without hindering business operations). Of course, having mobile device management in place to approve and secure new devices is key, as is multi-factor authentication, wherever it can be implemented. You should have a security policy that is clear enough that users - be they the CEO or a new entry-level employee - know what their responsibilities are when they use the device, and/or access the network. ***TIP: Consider disabling unwanted connection ports, such as USB sockets. This can be done using cheap blanking plates, or by disconnecting the ports internally, and prevents connection of unwanted physical devices.***

14	Have you renamed or disabled default accounts and passwords for all devices, services and software, including IoT devices (e.g. smart white goods, wearables, digital assistants, etc.)? **PR.AC**	Default administrator accounts and passwords are a major risk point, especially common in "Internet of Things" devices. Often created by companies specialising in the hardware side with limited experience or expertise in software or security, IoT devices are often found to have extremely weak privacy and security, with some hardware proving impossible to update when vulnerabilities are discovered. As connected devices become more common, businesses need to carefully review the kit they plan to acquire, making sure it not only performs its key function properly, but does so in a secure and manageable way. Selecting based on brand is less of a guarantee of quality in this area, as some large firms may simply bolt internet connections on to their existing product lines with little thought for the security implications. This makes it all the more important that factors like ease of updating and control of login accounts are checked for compliance with security standards. Once a device has been acquired, any built-in accounts, especially those with admin rights, are likely to be readily available online. Set up your own accounts with strong passwords, and disable any built-in ones, before connecting the device to any important networks. ***TIP: When connecting smart devices within an office setting, consider using a segregated wifi or wired network which is kept separate from your key business network and data. If the device only requires access out to the internet and does not need to connect directly to anything internal, this segregation can hugely reduce the risk from poorly-secured devices.***
15	Do you allow "Bring Your Own Device" (BYOD) at your organization and if so, do you have an up—to—date policy to manage and control their access to your services and data? **PR.AC**	Bring your own device (BYOD) is not a recommended approach to security, but truth be told, we know that many companies rely on users' personal equipment. This can be due to users preferring to use their own devices rather than company-provided machines. It could also simply be a cost-saving exercise - both valid reasons, but operating with BYOD does increase your cyber risk. If you do allow personal devices to connect to your network and access your organization's online systems, services and data, it is strongly recommended to have an up to date BYOD policy to control what devices can access what services. The policy should also tell users what security protocols and procedures they need to follow in order to use a specific device to access the network. For example, you might only authorize access to the network from personal devices that have specific security services installed (e.g. VPN, encryption, back up, firewall, anti-malware, password manager, etc), all controlled by centralized mobile device management. Being able to manage devices remotely and securely is key. For instance, Acronis Cyber Protect, with its single interface across all its services, can radically simplify remote device management. ***TIP: Always aim to grant the least amount of access rights possible, without impacting business growth.***

16	Do you allow users to access your network remotely (e.g. from home or while travelling), and are you confident the connection is properly authenticated, encrypted, and tracked? **PR.AC**	The benefits of having a remote working and device policy, allowing users to access the network and its data regardless of their location, can be huge. Aside from providing flexibility during crises when workers are unable to travel to offices, remote access can also reduce the environmental and time impact of commuting, and allows workers the freedom to fit in work around other commitments, improving job satisfaction and ultimately productivity. It can also be vital when a key worker's input is needed but they are not able to attend the office due to travel or other commitments. Depending on your policy, some users will be accessing the network from their own devices, while others will be using company-owned hardware. Either way, it's crucial to ensure all devices accessing your networks and data are known and trusted, ideally centrally managed with enforceable protections conforming to your core security policies. Make sure secure authentication is required to access your network, track what devices are connecting and when, and block all unapproved and unmanaged devices. ***TIP: Make sure any mobile device management software is properly configured to allow remote location tracking and remote wiping of devices, in case something which could be storing company data gets mislaid or stolen.***
17	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. 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. ***TIP: Complete oversight of your network is key to ensure the systems are healthy and running smoothly, but too much information can be worse. Set your console to provide the right level of information for your needs.***



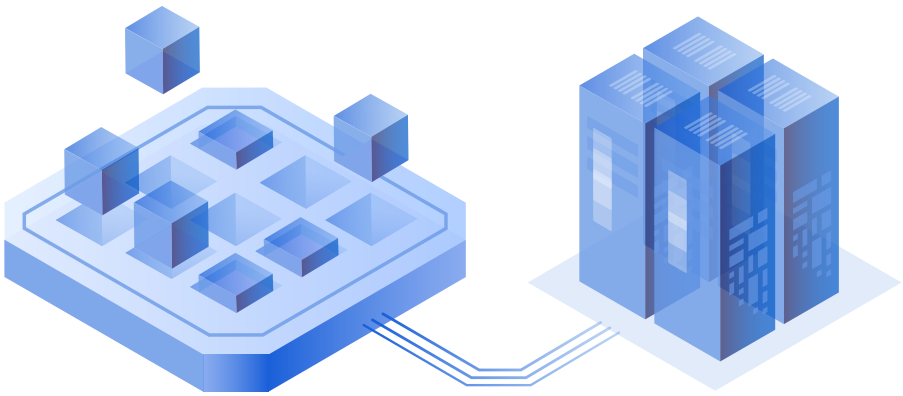
18	If you provide guest access to your networks, do you provide segregation from your critical systems and sensitive data? **PR. AC**	Providing business visitors and customers with access to the internet brings many benefits, but if you do not secure guest internet access for business visitors you will be exposing yourself – and them – to considerable risk. Segmenting your network is important for a few reasons. It stops visitors gaining access to parts of the network used by your employees for business operations. Guest users should not be able to see confidential files and resources. **Recommendations include:** • Set up a second SSID specifically for guests to use to stop guest users to access your internal WiFi network, and make sure it is password protected. • Choose the SSID name wisely – so that it does not advertise the fact that the network belongs to your business. This will make it harder for hackers to attack your WiFi network. • Disable remote admin access on wireless networks – if a hacker succeeds in gaining access to your WiFi network, this will limit the harm that can be caused. • Use a management solution that collects guest credentials so you can monitor guest behavior to ensure no one is trying to abuse the system. -Modern routers and access points support WPA2 encryption. Make sure this is enabled – or WPA3 if it is supported. ***TIP: In the event of a malware or ransomware infection, a segregated network can be very effective in limiting the harm caused.***
19	If you are storing any data in the cloud (e.g. AWS, Google, Office 365, etc.), have you used all available tools and best practices to harden its security? **PR.AC, PR.DS**	How many times have we read about a company, even those boasting a strong reputation, who've accidentally left their online cloud database, full of PII, for all and sundry to find? In some of these cases, the organization has been lucky and gets a chance to harden its security against unauthorized access before anything gets stolen. Others however have been dragged through the press for leaving sensitive information about employees, customers, services or business partners open for anyone who happens to land on the page. • Set up role-based access and permissions for accessing all your cloud resources, and even your database instances. • During transit, your data is vulnerable to failures, outages or attacks that may result in data loss or cause compliance issues. Make sure you secure the data by encrypting in transit and at rest. • Make sure to back up all the information for optimum security. ***TIP: Default configuration is rarely designed to offer optimal security. It is often balanced between some security and additional services. It is vital to read through all the configurations and assess if the settings meet your particular organization's requirements.***

20	Do you track all systems, services, users, and contact lists to ensure anything unwanted or expired is deactivated or disabled? **PR.AC, 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, but in some cases, you will even need to notify the authorities, especially if user account information might have been accessed by an unexpected user. Regularly reviewing the network to see what systems, services, and users are currently authorized is highly recommended. A key question is this: Do any accounts need to be removed? Added? Permissions 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 significantly reduce the complexity of a network. These reviews, done regularly, can reduce your threat exposure dramatically. Integrated management software like Acronis Cyber Protect can 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. ***TIP: Set an expected expiry date for all services, systems and accounts at creation time, reviewing as that date approaches and only extending it for as long as required.***
21	Are all users given regular cybersecurity awareness information and training, covering how to avoid the latest threats (e.g. 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 defence, underpinning your security services. Most people 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 each of 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 the information or access rights they possess must be properly guarded will go a long way to safeguard your network environment. Cyber awareness training should be provided regularly 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 is a proven method to help defend the network, and the organization, from headaches. TIP: Talk to users about improving personal security, using ID theft as a case study. This approach will help engage them with the issue by applying it to their own lives. Then you can show how these security lessons can apply to safeguarding the organization.

22	Do you perform regular staff testing to identify poor security practices (e.g. simulated phishing attacks)? **PR.AT**	A strong first line defence is key to mitigating against an attack. Social engineering has proven a highly successful route for cyber criminals to get inside an organization. All it takes is one employee to give away their credentials accidentally, potentially giving the social engineer attacker the keys to your organizational kingdom. To help mitigate against social engineering attacks - attacks where the attack dupes the victim into parting with login credentials, names of secret files, personal contact information - you need to have wary and educated users. Educating users is not always easy. Imagine trying to explain how a car functions to an average driver - most are not interested. However, by making the training personal, you can reach a new level of understanding. For example, talk about how an attacker might try to trick a user to access their personal bank account or picture folders. And then share the steps to mitigate against such an attack. This approach goes a long way to help them be much wary in an organizational environment. Once you have given the appropriate training, you can test its success. Often, simulations are run before and after a training session to see if users have evolved their online behavior to exercise more caution. Running phishing exercises, or planting pretend offsite workers to see what information they can garner by wandering around the office, can help you understand your REAL operational risk. Of course it is important afterwards to review the findings, tighten security where necessary and repeat training for any users that effectively "failed" the simulation. The point here is not to call them out, but to ensure they have the training they need to be a strong first line of defense. ***TIP: Simulations are very useful. Try to run them even in small environments at least every six to twelve months for maximum return on investment.***
23	Do you encrypt all sensitive traffic? **PR.DS**	Securing data in transfer is important not only through public networks but also in private networks. The data has to be protected if it is business critical or if modification or interception could lead to a security incident. Keeping the data secure means ensuring the principle of the CIA triad (Confidentiality, Integrity and Availability). This is an important concept in information security. If there is a possibility that data will be modified during the transfer to the final destination, the CIA principle is not ensured. Where a device that can access sensitive information is reachable via a web interface, web traffic must be transmitted over Secure Sockets Layer (SSL), using strong security protocols, such as Transport Layer Security (TLS). Sensitive data transmitted over email should be secured using cryptographically strong email encryption tools such as PGP or S/MIME. Or, prior to sending the email, the user should encrypt covered data using compliant file encryption tools and attach the encrypted file to email for transmission. ***TIP: Strong encryption can consume more CPU resources than weak encryption. So make sure you find an encryption solution that best meets the needs of the organization, and the information it is trying to protect, all without negatively impacting performance.***

24	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, and far too much of it is not properly encrypted. 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. ***TIP: Using a centrally-managed encryption system can help reduce the danger of data being lost or inaccessible due to forgotten passwords, or key users being unavailable.***
25	Do you have a reliable and regularly—tested backup and restore strategy for all important data and systems, with appropriate duplication and diversity of storage? **PR.DS**	**Keeping secure and reliable backups of all vital data and systems is a key step in any cybersecurity process. Following these guidelines will ensure that you cannot be taken offline by a ransomware attack that encrypts data, effectively holding it ransom until the attackers get what they want:** • Keep at least three separate copies of your data (so no single event will destroy all copies). • Store the data in at least two different formats (i.e. disk, tape, cloud, etc.). • Keep one copy offsite to protect against fire, flood, theft, and other physical disasters. And don't think that typical cloud storage (e.g. like that provided by Google Drive or Dropbox) and backup storage are the same thing - they aren't. A true cloud backup service enables you to create automated backups of complete systems and store as many versions of backups as you need. Leading backup solutions like that from Acronis come with a stellar reputation from users and industry analysts alike. The new Acronis Cyber Protect solution integrates its backup functionality into its unique AI-enhanced Data Protection with Cybersecurity offerings, simplifying the management of information security across the organization. ***TIP: Remember what back-ups are for. Making backups and keeping them safe is only the first step - the important part is reinstating your environment after an unforeseen event. Being able to quickly and easily restore important data is key - make sure to document and test this process regularly to make sure nothing is preventing a speedy return to a trusted state.***

26	Do you monitor all data leaving your devices and networks to prevent unwanted leaks (e.g. being copied to USB sticks)? **PR.DS**	**Keeping logs to uncover what data is leaving the organization is a very important step to preventing data leaks. There are number of ways data can leave an organization:** • a cyber event led by an unknown attack agent; • an employee who's accepted a job at a competing firm; • a disgruntled employee wanting to cause trouble for the organization; and • an "unhappy accident" where a user has inappropriate access rights to information they should not be viewing (e.g. remuneration information). By keeping records of all data, and when it is added, edited, or deleted - along with the username and timestamp - lets you both monitor for suspicious or unwanted activity. Should the worst happen and you find yourself a victim of a leak, it gives you the information to track where the breach happened and outline what was taken. It also provides necessary authorities with the right information, and such information can go a long way to finding out where the attack stemmed from. ***TIP: Ensure to set up alerts so that when unusual, suspicious or unwanted activity takes place, you have a better chance of preventing the behavior from being completed.***
27	Are all devices and storage media properly encrypted and secured against unwanted access or theft? **PR.DS**	Any organization here who says yes, without any tools to help them monitor and review current network access status, must be fibbing. These days, people can carry around wearables, mini usb-c devices, and other IoT devices which are provided by the organization. Make sure you protect these devices, which are easily portable and easily lost. If they end up in the wrong hands, no information should be retrievable without proper authorization. ***TIP: Keep an inventory that is regularly reviewed of all devices and storage media that has been vetted and approved for network access.***



28	Have you properly documented and regulated which users require access to which systems, data and other services (following the principle of least privilege)? **PR.IP**	The principle of least privilege means granting access only to that which is needed, and no more. Security policies should not prevent anyone from getting hold of information, or making use of systems, which are vital to the performance of their work, but should equally not allow anyone to access anything not strictly required. Applying such an approach in a flexible and efficient manner requires keeping track of exactly who needs access to what. Tracking this matrix of information, and ensuring it keeps up to date with changes in staffing and business practices, is a complex and resource-intensive task. The most common way to simplify this is to use groups, each with their own sets of rights. A user is assigned to a group as required. This means you need to consider your group formation very carefully, and be open to reviewing it regularly so that it does not cause a bottleneck in IT services. Maintaining your user accounts and groups can be made more efficient by using centralized management software with full visibility of all your users and systems in a single interface, like that found in Acronis Cyber Protect. ***TIP: A clear and simple naming convention, for both users and devices, can help keep track of things. To further minimize confusion, make sure to use separate top-level groups for users, workstations, servers, and other device types.***
29	Have you accurately documented your security procedures and policies and involved all the appropriate parties, including external business partners and the supply chain? **PR.IP**	Many organizations rely upon suppliers to deliver products, systems, and services. You probably have a number of suppliers yourself. But supply chains can be large and complex, involving many suppliers doing many different things. Yet a vulnerable supply chain can cause damage and disruption. Damaging attacks on companies have demonstrated that attackers have both the intent and ability to exploit vulnerabilities in supply chain security. This trend is real and growing. **You would be surprised at how few organization could list the following without having to go digging:** • Who is in your supply chain? • What does their individual security look like? Is it mature or practically non-existent? • How do your suppliers manage their own supply chains, as their failure may impact you? By setting minimum security requirements that your supply chain must meet in order to do business with you, you can significantly improve your security posture. ***TIP: Be strategic. Contracts that provide basic commodities such as stationery, or cleaning services require entirely different approaches to information security management to those that provide critical services.***

30	Do you track that all Operating System, device firmware, software and security patches are up-to-date and automatically updated where appropriate? **PR.MA**	No complex software is perfect, and the more complicated something becomes, the more likely it is that flaws and vulnerabilities will eventually be found in it. Regular patching ensures that problems are fixed as early as possible, minimizing the exposure to potential threats. Keeping on top of all the software running in a business is a major task, especially when you also need to align what you have installed with new versions and patches being released at often unpredictable schedules. When major new vulnerabilities emerge, patches can be released very quickly, but new threats exploiting those vulnerabilities can come out very rapidly too. Getting those patches in place immediately keeps you safe from these emerging threats. Centralized monitoring and management of software versions and patch levels across your environment can massively reduce the workload of keeping track. Leading providers like Acronis Cyber Protect can even manage patch levels inside backups of systems, ensuring that if a server or a user's desktop has to be restored, it comes back online with all the latest patches and updates. ***TIP: Subscribe to reputable alerts on emerging vulnerabilities and patches that affect your key software and tools to get an early alert of potential problems.***
31	Do you have fully operational, correctly configured, patched and updated firewalls on your endpoint devices and at your network perimeter? **PR.PT**	Client (or endpoint) firewalls make use of policies and rules to allow or block unwanted network traffic. Unfortunately, firewalls come in all shapes and sizes, each touting to be the best. With a reputable firewall, an administrator can choose to be in charge of its configuration, or give the user the rights to manage the client firewall settings, as it suits your organization's requirements. In order to be effective, they need to be installed and properly configured on every device and at the network's perimeter. Ideally, a client firewall blocks user access to sites and services that have unusual, unexpected or unwanted behavior. Many reputable firewalls also allow for content filtering, allowing the administrator to quarantine or block specific information from leaving the company - a great resource if a disgruntled employee tries to copy over your entire customer account list. The tighter the controls over ports and services, the lower your overall risk level. ***TIP: Make sure your firewalls are properly configured and operational with regular penetration testing.***

32	Do you have up-to-date, 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 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. It can also let you roll out changes to policies as your business needs evolve and new types of threat emerge. Best-of-breed providers like Acronis Cyber Protect include on-access and on-demand malware detection both locally and in the cloud. 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. ***TIP: Avoid using real (and potentially dangerous) malware files to verify your protection is working - try the free, safe simulators provided by organizations like EICAR and AMTSO.***
33	Is your email traffic being scanned to remove any malware, spam, phishing attacks, and other unwanted content? **PR.PT**	Email remains a primary vector for scammers to dupe users into falling for a popular threat, be it a phishing attack, a malvertising stunt, or a ransomware attack. Scanning your email for threats before it lands in your users' inboxes will boost your security posture measurably. While no solution is perfect, a few will provide excellent protection, blocking all known threats as well as new, previously unseen threats by relying on behavior analytics. This refers to the security software looking at thousands of tiny behaviors and if too many are unpredictable, it slams the dodgy components of the email - its attachment for instance- into quarantine for further review. Many cloud services provide a built-in email traffic filter to help reduce the amount of unwanted mail, but if you have a strong front line reliant upon email communications running smoothly, it is worth considering adding an additional layer of email protection to further reduce the risk. ***TIP: Set your mail filters to automatically block any file types you definitely have no need to be sending or receiving via email - for example, few organizations need to be able to transfer executables this way. Automatic blocking can significantly reduce scanning time and increase throughput.***

34	Is your web traffic being scanned to detect and block malicious, fraudulent, distracting or unwanted traffic? **PR.PT**	In terms of cybersecurity, the web is both a vital resource and a major risk point. While many workers' roles rely on internet access to communicate, find information or simply operate their tools, that same internet is the source of most potential dangers and the pathway of most data leaks. It's therefore vital to ensure that this key data vector remains fully accessible to everyone who needs it, while preventing any unwanted inbound or outbound traffic. Web filters do this by analysing all traffic, looking at everything from the content itself to the data types and protocols in use. They may also check the source and destination points involved to help decide whether the traffic in question is approved or undesirable. Web filtering acts as a first line of defence against malware infection. By blocking all access to known-bad or even suspicious URLs, a large portion of the malware threat is immediately prevented; no matter how sophisticated or hard-to-detect a piece of malware is, it presents little threat if the webpage pushing it is completely sealed off from your environment. For optimum efficiency, look for a solution which combines this sort of filtering with multiple other security features in a single simple control interface, like Acronis Cyber Protect. ***TIP: In some circumstances, more complex filtering can prevent access to gaming, gambling, porn or even social media sites. Depending on your environment, it may be suitable to reduce employee distraction, but these filters can be prone to both gaps in prevention and false positives, frustrating employees and reducing efficiency. If such additional filters are required, be sure to educate users on the reasons for blocking such content, and on how to report inappropriate blocking.***
35	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 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 defence. 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 data that is in regular use, data being archived, and the content of backups themselves. 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 quickly. Leading providers like Acronis Cyber Protect which integrate backup and malware-detection functions can make this process simple and efficient. ***TIP: Consider scanning your storage with a secondary anti-malware product on a regular schedule, for a belt-and-braces approach.***

36	Do you have systems in place to ensure that all external services you provide (including websites, web applications and databases, remote login systems, etc.) are resilient to traffic spikes and distributed denial—of—service (DDoS) attacks? **PR.PT**	Pretty much everything has some sort of upper limit to the amount of work it can do before the cracks start to show. Network infrastructure tends to be designed to be able to handle much more than the everyday baseline usage, so small upturns in activity can be handled with no issues. But once something is exposed to the internet, these calculations become much more difficult. Sudden surges in traffic can come without warning, whether they're intentional (an adversary deliberately flooding you with traffic to try to knock you offline) or entirely accidental (a trending new app or website has a name similar to your company or product, and you end up getting a glut of visits from the world's more confused and typo-prone users). Internal measures, such as load-balancing between multiple servers, can provide some support for lower-risk or low-exposure systems, but for most internet-facing services, especially websites, a third-party content delivery network (CDN) is the most effective method of protecting against traffic spikes. These distributed networks have huge numbers of connections to the internet spread all around the globe, sharing your traffic between them to prevent any bottlenecks. ***TIP: While many free CDNs are available, paying for a fully supported option may come with a range of additional benefits, such as improved speeds or assistance with recovery from incidents.***
37	Do you monitor for insider threats, such as analyzing user activity to spot any anomalous behavior (e.g. logging in from an unusual location, accessing unauthorized files, etc.)? **PR.PT**	Bad digital actors rarely like to announce their presence until their tasks are done. Once they have a route into a network, they will tiptoe, effectively cloaking their presence. An administrator who has intimate knowledge of the network activity, and has configured the tools to alert when unwanted, suspicious or unusual behavior is spotted, is much better positioned to stop an attack dead in its tracks. Not only will you have the right information to inform stakeholders on what has happened, but you are much less likely to be accused of taking your finger off the network pulse. As an added bonus, you are more likely to have pertinent information to share with the authorities, which may lead to an arrest. ***TIP: If you use behavior-tracking software to flag up unexpected activity, be sure to train it properly for your environment - you don't want the boss's planned trip to China to sound alarms.***

38	Do you ensure regular penetration tests, including vulnerability scans, are performed across all your systems, networks, and services (including third—party and cloud—based services)? **PR.PT**	A key part of securing your systems and data is regularly testing that your protections are in place and properly functioning. Penetration tests exercise various aspects of your networks, systems and even personnel, to make sure that physical, software and hardware protections are operating properly, processes are being followed and no gaps can be found in your attack surface. This includes regularly checking for new vulnerabilities in any tools or systems you may be using. Bad actors are extremely fast at jumping on any newly-discovered vulnerability and making use of it to compromise affected systems, so rapid detection and patching is vital to keep your data and services secure. Keeping track of your entire estate of software and operating systems, and making sure they're kept up to date, can be a resource-intensive task. Quality patch management software like that included as part of Acronis's Cyber Protect solution can automate the patching process, significantly reducing this overhead. ***TIP: In the case of "zero-day" vulnerabilities, which have been discovered but for which patches or fixes have not yet been made available, workarounds should be found to keep things running while minimizing the exposure until a proper fix comes online.***
39	Do you employ a defence—in—depth approach to cybersecurity, e.g. multiple layers of security controls throughout your network and services? **PR.PT**	Defence in depth is the belt-and-braces approach to security, covering every potential vector for unwanted intrusion or compromise with multiple protective layers so that if one is breached, there are additional barriers in place. This might be something as simple as running malware detection from multiple different providers at different layers, such as the network edge and on endpoints, so that if an item is not spotted by the perimeter scanning there is a better chance of it being picked up and blocked when it reaches a user's system. It could also include requiring approval from multiple team members for a major action, such as a transfer of funds, reducing the chances of a sneaky spear phishing attack tricking someone into handing over cash to a scammer. ***TIP: Think about every process and protective tool and look out for potential single points of failure - these should be backed up by extra layers to minimize risk.***

40	Are you aware of any systems or devices in your environment that cannot be patched or updated? **PR.PT**	Eventually, everything needs some sort of updating, patching or other general maintenance. Best practice dictates that all updates and fixes should be applied as early as possible, after careful testing in the case of mission-critical systems. Some things, however, are difficult or even impossible to patch. This might be a creaky old machine, long out of official support but which serves a crucial purpose, running some bespoke software which cannot be ported to a more modern platform. Or it might be a shiny new IoT device whose makers omitted to include any way of applying updates. Either way, if there are potential security vulnerabilities, they need to be addressed somehow. First, make sure you know which devices are lacking patches, and exactly what risks this leaves you exposed to. These risks need to be weighed against the importance of the system in question - is the pain of replacing the system with something more modern and resilient greater than the potential nightmare of having it compromised, any data it holds leaked, or even used as a stepping-stone to get access into the rest of your networks? Keeping track of all potentially vulnerable systems and devices, and the related risks, will help you keep on top of this balancing act, and let you retire old devices as soon as the risk becomes greater than their importance to your business. ***TIP: If replacement is not an option, there are usually some mitigations you can put in place to limit your exposure. Keeping such "zombie" systems in a segregated network, well away from your key systems and services, is often a good first step.***
DETECT		
	Q	**A**
41	Have you an automated alert system to inform key IT personnel of unwanted behavior or activity on the network? **DE.AE**	Most security monitoring systems are constantly active, always on the look-out for indicators of potential danger. If the alerts they push out are only reviewed manually, for example when the person tasked with maintaining IT security is on duty and has time for this work, there can be a sizable gap between the warning flags being raised and action being taken. Automated alerting, going out to everyone who needs to know about these things, is vital to minimize the gap between detection by systems and any manual intervention required to prevent a problem getting any bigger. It's also important to ensure duties are properly shared and distributed, so an alert isn't missed because the lead person is unavailable. ***TIP: Consider regularly testing your alerting system to check messages are getting through, and requiring a response from recipients to confirm this.***

42	Do you regularly review the output from your security systems — anti—malware, firewall, IDS, traffic filters, etc. — to spot unwanted behaviors 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 common scenario. 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. It can help a lot if your main security monitoring tasks are combined in a single central management system, like Acronis Cyber Protect. ***TIP: If reviewing duties are shared among multiple staff, keep a simple tracker which each member updates when the day's reviewing tasks are completed. This helps avoid duplication of effort, and can flag up when a staff member is failing to fully review information.***
43	Are your security monitoring systems correctly configured to produce accurate, informative and easily accessible logs? **DE.DP**	Monitoring systems come in all shapes and sizes. Not all will meet your needs. Some might even introduce more complexity to information system management - not what any company wants to hear. To get the right tools that will both be cost effective and useful, you need to have a clear understanding of your objectives as an organization, as well as be aware of the legal and industry security information requirements that impact your organization. And this is where logs come in. Not only can they help you track down and stop unwanted or questionable behavior, but logs are invaluable resources to understand how your network services its users and where efficiencies and productivity improvements can be made. But this is only true if the logs are easy to understand and parse. Otherwise, it can be a needle in the haystack job - not fun for anyone. Make sure you review how logs are accessed and used before you purchase any security monitoring tools. Use a few scenarios to see how long it would take you to access a specific log to get key information. Reputable security providers like Acronis offer continuous data protection, ensuring that users will not lose their data, including logs. ***TIP: Make sure you have a plan B, should the logs somehow get corrupted (e.g. back them to a separate location and/or a physical drive).***

44	Do you secure your logs (using encryption, archiving, reliable backups, tamper prevention) as well as monitoring their access? **DE.DP**	Some security solutions produce vast amounts of log data, enabling fine-grained review of huge quantities of tiny events. This data can be overwhelming in real time, and is best automatically processed and parsed. That way, important incidents are flagged up. But the remaining data also has a crucial role to play. It is extremely useful for post-incident analysis, to get a clear picture of exactly what happened and what might need addressing to circumvent future similar incidents. In some cases, there are legal requirements covering what data needs to be retained, and for how long. Keeping logs well protected and backed up ensures these requirements can be met. The content of logs may be sensitive and should be kept away from those not authorised to see it. Not only is it vital to control who can access the logs, limiting to only those who have a pertinent role to play. You want to prevent unwanted viewing or changing of log data. ***TIP: There's always the possibility that those behind an incident may try to cover their traces by doctoring or deleting logs, so all access needs to be tracked and recorded so that any changes made by a malicious insider, or an attacker using stolen credentials, can be rolled back to a known-trusted state.***
RESPOND		
	Q	**A**
45	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 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 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.***

46	Does your incident response plan include coordinating with your business partners, users, customers and where necessary law enforcement? **RS.CO**	No business operates in a vacuum. There will always be at least some customers, partners, suppliers, regulators, auditors and others who interact with your business, and when a cybersecurity incident targets you, there may well be an impact on some or all of these groups. It's vital that your incident response plan includes any required communications with these third parties, making sure they are kept informed of how the incident (or the cleanup process) may affect them. ***TIP: Keep contact details of key people and teams alongside or within the incident plan documentation for easy access.***
47	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 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 correctly 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		
	Q	A
48	Should a cybersecurity event take place, can you ensure that any restoration processes are properly coordinated with affected partners, users, customers and law enforcement? **RC.CO**	When you're busy trying to get your business back into shape after a damaging attack or incident, it's easy to focus only on your internal needs; it's your business that has been mainly impacted, after all. But in many cases there will be third parties who may be as much affected by the recovery process as by the incident itself, and it's important to keep them in the loop so they know what to expect. For example, if your website has customer accounts which need to be rolled back to a trusted state, you may need to inform customers that any changes made recently may be lost. If law enforcement or third-party investigators are involved, they may need to have access to the pre-recovery state of your systems and data for their investigations, so you need to talk to them to ensure they're ready for the restoration to happen. Keeping details of all potentially affected parties on hand, perhaps within or alongside your incident response policy, will help you ensure that all the right people get the right information, and aren't taken by surprise when you restore or roll back your systems and data. ***TIP: Remember to review your State's and federal legislation on computer incidents and make sure you inform the right authorities where necessary. There is little sympathy for the organization which tries to hide an incident from affected parties, let alone the authorities, and playing the I-didn't-know-card will not get you very far.***
49	Does your incident response policy include a post—mortem plan so that you can learn from a cybersecurity event and incorporate any lessons learned? **RC IM**	In the aftermath of an outage or compromise, once everything has been cleaned up and restored to normal working order, it's tempting to sit back and relax after a hectic and stressful time, putting the incident behind you. But this is an important time to reflect and review the entire incident, flagging up any snags or gaps in your security and recovery processes which could have made things worse, so that if there is ever a "next time", you are as well-prepared as possible. The plan needs to evolve with your environment and the threats that it faces. It needs to be up to date. A three-year old plan will not have the right contact details, procedures, policy references, etc. It could even cause more confusion than the actual incident. ***TIP: Try walking through your incident response plan and rating how well each step was performed, and noting whether anything could have been done better (or more quickly). Take these learnings and roll them into the next version of your plan.***

50	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 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. 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. ***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.***

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 This Tool To Work

Don't forget that Acronis has a customizable, Word doc version of this questionnaire that you can white label and use with your clients.

Copyright © 2002–2020 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2020-05