20 Questions That Could Save Your Business

Cybersecurity And Cybercompliance Self-Assessment Guide

Thank you for taking the time to complete this self-administered assessment of your organization's exposure to cybersecurity and cybercompliance risk. The purpose of this guide is to help you discover likely weaknesses in your defense against common threats to your organization's operational and financial health.

This guide is not a substitute for a rigorous technical analysis of your network, systems, user behaviors, and cyberdefenses. However, your answers to the 20 carefully selected questions in this guide should quickly help you understand where you can most likely benefit from an investment in better risk management. Here they are:

1: Does your company utilize multifactor authentication (MFA)?

MFA is the use of two or more factors to grant a user access to a resource. For example, in addition to requiring a password, a system may send a one-time numerical passcode to a user's smartphone that they then have to type into a challenge screen. Or a system may require an additional biometric identifier such as a fingerprint or facial recognition.

0	1	2	3	4	Score
We never use MFA		We use MFA for a few key systems		We use MFA everywhere	

2: Does your company have strong password policy and controls?

Strong password policies include requirements on the length of passwords (at least eight characters), characters (at least one number and one other mark), rotation (e.g., quarterly), prohibition of reuse. Strong password controls are the mechanisms you use to make sure that users' passwords do in fact meet your criteria for strength, rotation, and non-reuse.

0	1	2	3	4	
We have no policies or controls		We have some policies but no controls		We use a password manager to ensure password strength	

3: How does your company install software security updates?

The security community is constantly discovering vulnerabilities in popular software products, which are then publicly announced as a Common Vulnerabilities and Exposure (CVE). So software companies are constantly issuing security "patches" to address those CVEs. The longer it takes your IT team to install those patches, the longer you remain vulnerable to attackers who constantly search for and exploit CVEs wherever they find them.

0	1	2	3	4	Score
No set process for identifying and fixing CVEs		We have a 30-day backlog of patches we need to install		We actively track CVEs and are currently up to date	

4: How are access privileges revoked from terminated employees?

Your current employees have lots of access to your data and systems. So when you terminate an employee, it's important to revoke all of those access privileges. This is especially true in the case of a disgruntled employee who may want to do harm to your company as an act of revenge—or one who goes to work for one of your competitors.

0	1	2	3	4	
No set process for revoking privileges upon termination		IT is alerted and revokes privileges manually		All privileges revoked completely and immediately	

5: How does your company train users to resist "phishing" attacks?

Cybercriminals commonly penetrate an organization's cyberdefenses by tricking users with fake emails and/or deceptive phone calls ("phishing"). One of the most important ways organizations protect themselves against these social-engineering tactics is to train their users in best practices for safe computing. The safest organizations also perform simulated phishing attempts on themselves to see if the training has been effective.

0	1	2	3	4	
We don't do any phishing-related training		We have sent some info to employees		We regularly train and test our people	

6: How does your company detect and stop digital intruders?

Getting hacked or phished doesn't have to spell disaster for your company IF you can detect and interdict malicious activity inside your network before the invader can reach your most valuable data and systems. But to do that, you must have a reliable way of detecting indicators of suspicious activity in your environment. And you must be able to respond to the detection of such threats quickly and decisively.

0	1	2	3	4	
We don't have tools that detect active threats		We have endpoint detection and response (EDR)		We have extended detection and response (XDR)	

7: Does your company segment administrative privileges?

The administrators of your IT systems (sysadmins) have the most far-reaching privileges in your organization. And they need those privileges to perform their everyday technical tasks. But if a hacker gets hold of those sysadmin credentials—which they invariably try to do—they can do virtually unlimited damage. That's why it's essential to limit the damage hackers can do by making sure no single administrative credential can grant them access to everything.

0	1	2	3	4	Score
Our admin(s) use the same password everywhere		Our admin(s) try to use a few different passwords		We fully segment all admin privileges	

8: How do you make sure your firewall is optimally configured?

Your firewall is a key component of your cyberdefense—ideally capable of blocking any unauthorized network traffic while not blocking any traffic that your people need to be productive. But it's not easy to achieve that balance. Any hackers will take advantage of any gaps in your firewall protection. So smart companies regularly test their firewalls from the outside (penetration testing) to find gaps and fix them before the bad guys do.

0	1	2	3	4	
We never get penetration tests		We've had some tests, but it's been a while		We test our firewall regularly, like clockwork	

9: Are you optimizing your risk profile for cyberinsurance?

Cyberinsurance provides vital financial protections from the consequences of a cyberattack or other technology-related business interruption. But due to unsustainable losses, insurers are adopting increasingly stringent underwriting policies. To qualify for the right coverage at the right price, organizations must therefore be able to demonstrate that they have taken steps to minimize their prospective insurer's exposure to risk.

0	1	2	3	4	
We do not have a true cyberinsurance policy		Our policy and premiums are based on our current posture		We actively seek to qualify for the best coverage at the best price	

10: What's your company's backup plan?

Your backup files can be your last line of defense against a costly, extended business interruption. But it's not enough to just copy your files. You must ensure that you could actually restore those files successfully to production-readiness if you needed to. You must make sure you're backing up the files you need as often as you need to. And you must make sure that hackers can't get to those backup files at the same time as they attack the rest of your business.

0	1	2	3	4	
We perform backups and that's about it		We have good backup files and occasionally test them		We regularly test our backups against Recovery Time Objectives (RTO)	

11: Do you subject your vendors to cybersecurity requirements?

Once cyberattackers succeed in compromising one organization, they often use that beachhead to launch attacks on other adjacent organizations. So if you do business with companies that are lax when it comes to cybersecurity, they are putting you—and your customers—at risk every day. The solution, of course, is to set some minimum standards for your vendors—and to require them to provide some documentary evidence that they are in fact fulfilling those standards.

0	1	2	3	4	Score
We don't ask vendors about their cybersecurity		We only ask them about security as it relates to their direct dealings with us		We have specific cybersecurity requirements for our vendors	

12: How are you securing your use of the cloud?

Cloud-based applications and services offer compelling value by allowing your organization to acquire new digital capabilities without the additional capital and operational expenses associated with deploying more IT infrastructure internally. But your cloud providers are not responsible for your security and compliance. You are.

0	1	2	3	4	
We trust cloud providers to keep us safe		We have put some cloud protections in place		We actively manage all cloud-related cyberrisk	

13: How are you managing your physical security?

Cybersecurity isn't just about keeping criminals from hacking you over the internet. It's also about keeping them from getting to your sensitive data and critical systems by more ordinary means, such as simply sticking a thumb drive into an open USB port. To maintain this physical security, organizations must control physical access with the same rigor as they do digital access.

0	1	2	3	4	
We keep an eye on whoever enters our office		We restrict access to our server room		We have policies and controls for rooms, USB drives, hard copies, etc.	

14: Do your employees email sensitive information "in the clear?"

Business email compromise (BEC) is a common occurrence—which is just one reason that your employees should never transmit sensitive data such as Social Security numbers and banking information as plain text in their unencrypted emails. Organizations can prevent this from happening by implementing a number of measures that include employee training, email encryption, recipient authentication, and data loss prevention (DLP) technologies.

0	1	2	3	4	
We have no way to prevent risky emailing		We give employees the ability to encrypt sensitive emails		We have policies and controls for email content and encryption	

15: How does your company address cybercompliance mandates?

Just about every company is subject to regulatory mandates regarding the way it manages data. For companies that handle credit cards, that mandate is PCI. For healthcare, it's HIPAA. For financial services, it's SEC and FTC guidelines. Compliance with these mandates requires that companies implement specific types of cybercontrols. Compliance also requires that companies be able to document their implementation of those controls to auditors.

0	1	2	3	4	Score
We don't currently comply with any mandates		We are starting our cybercompliance journey		We have a full cybercompliance program in place	

16: Have you implemented special protections for special data?

Every bit and byte and every computer in your organization and every application you use in the cloud is data. But not all data is created equal. The flier announcing your next company picnic is not the same kind of data as the HR file where you keep all of your employees' Social Security numbers and ACH banking instructions. An effective risk mitigation strategy treats each of these data types appropriately in terms of access controls, encryption, backup, and other cybersecurity measures.

0	1	2	3	4	
We treat all of our data pretty equally		We have special protections for our most precious data		We have a multi-tiered approach driven by business risk	

17: How do you secure remote work and WFH employees?

Organizations increasingly depend on remote workers. Some of those remote workers are salespeople, field service workers, and other road warriors who need to stay productive wherever they are. Others are the new generation of work-from-home (WFH) workers who only come into the office when they need to. Any organization seeking to attract the best talent—and to keep that talent productive even if extreme weather or a natural disaster keeps them from coming to the office—therefore needs to safely enable remote work.

0	1	2	3	4	
Remote users only need their password		We use passwords and MFA to authenticate remote users		We have multi-layered safeguards for all remote logins	

18: Do you have an incident repose (IR) plan?

Despite all your precautions, your organization may still get hit by ransomware or some other type of cyberattack. But you can still significantly reduce the short- and long-term adverse impacts of those incidents by responding quickly and decisively. And your IR plan needs to encompass more than just restoring data from backups. It has to include pre-rehearsed processes for identifying and neutralizing the attack, communicating with employees via alternative channels, and making appropriate disclosures to customers.

0	1	2	3	4	
We don't currently have an IR plan in place		We have IR procedures for IT		We have a company-wide IR plan that we periodically rehearse	

19: Do you have a Chief Security Officer?

Effective cyberrisk management requires more than just installing some security tools. It requires strategic leadership to ensure that your security budget is being allocated wisely, that technology-related risks are proactively factored into executives' business decisions, and that your organization's security and cybercompliance posture is subject to the discipline and accountability needed for continuous improvement.

0	1	2	3	4	Score
We do not have a Chief Security Officer		Our technical security manager(s) try to think strategically		We have a true CSO or a virtual CSO (vCSO)	

20: How does your company view security and cybercompliance?

In an increasingly tech-centric world fraught with risk, effective security and cybercompliance are as central to an organization's performance as its human capital, its intellectual property, its go-to-market strategy, or its financial management. That's because security and compliance failures can permanently alienate customers, destroy brand reputation, and significantly diminish a company's valuation in the eyes of investors.

0	1	2	3	4	
"Security is unfortunately a necessary operational cost."		"Security is an investment that pays off in mitigated risk."		"Great security helps make us a great company."	

Self-Assessment Test Results

0 **Your Final Score**

Use the scale below as a starting point for taking actions that will raise your score—and, much more importantly, reduce your current exposure to risk while significantly improving your organization's future prospects.

Total	Assessment	Suggested Action
71 - 80	**Top performer** Your organization is among the elite 1% that have effectively optimized their operational mitigation of technology-related risk.	Keep doing what you're doing. Track new technologies. Review performance issues and budget allocation quarterly.
61 - 70	**Mature** Your organization is taking an effective, strategic approach to the mitigation of its exposure to both security and compliance risk.	Keep doing what you're doing. Come up with a concrete game plan for raising all your "3" scores up to "4" scores.
51 - 60	**Effective** Your organization is above average when it comes to cyberrisk mitigation but has some areas in need of serious improvement.	Keep doing what you're doing where you scored well while committing to raising your three lowest scores by next quarter.
41 - 50	**Vulnerable** Your organization is making significant investments in mitigation of cyberrisk yet is still unacceptably vulnerable to attack.	Get an independent assessment of your current security posture to make sure you target your primary shortcomings.
31 - 40	**High risk** Your organization has made a good start—but could easily suffer major adverse financial consequences from a cyberattack.	Substantially increase your investment in security and compliance. Engage outside resources to help you ASAP.
0 - 30	**Danger zone** Your organization is in immediate danger and could easily be put out of business tomorrow by even the most basic cyberattack	Call a managed security services provider (MSSP) or similar professional contractor to start fixing your problems now.

Marty Parker, Owner & CEO

843-699-1001