Seventy Questions to Assess Cybersecurity Risk on a Rapidly Changing Threat Landscape

Author: Patrick Barnett, CISA, CISM, CEH, CISSP, PCI QSA, PCIP
Date Published: 12 September 2023

SHARE

Some people may wonder why there are so many cyberincidents that take place. After all, in theory, everyone could follow a blueprint and design network security to be bulletproof. Unfortunately, there is no single method to make network security invincible—and there likely never will be. In fact, there is no pathway of actions that can be taken, money spent or technologies utilized that can remove all risk associated with cybersecurity. Sources and degrees of risk are constantly changing along with the threat landscape, and threat actors continue to deploy new techniques and utilize newly discovered vulnerabilities.

Cybersecurity Entropy

The cyberworld is akin to the concept of entropy[1] in physics. Entropy is a measure of the disorder of a system. The higher the entropy, the more disorganized the system becomes. Generally, with entropy, all things become less organized with time. This is certainly true when securing networks. Threat actors generally become more organized with time and there is a need to reduce risk just to keep pace.

Virtually every network experiences security entropy. Even if an enterprise has done everything possible to reduce risk, with time, more vulnerabilities (and resulting risk) are exposed. Data try to escape and things that have been stable become unstable—in other words, they experience entropy. Systems and security measures become less organized and more chaotic and are subjected to more entropy.

Even if an enterprise has done everything possible to reduce risk, with time, more vulnerabilities (and resulting risk) are exposed.

70 Layers of Defense

There are 70 questions that can be asked to determine whether an enterprise has most defensive principles covered and has taken steps to reduce risk (and entropy) associated with cybersecurity.

If you can answer "Yes" to the following 70 questions, then you have significantly reduced your cybersecurity risk. Even so, risk still exists, and entropy must be continuously monitored and mitigated. There is no specific number of layers that can remove all risk, just as there is nothing in the physical universe that does not experience entropy.

The following 70 questions are not ranked in any order:

Training
1. Do you conduct robust and frequent end user cybersecurity awareness training?
2. Have you taught everyone how to securely store passwords or passphrases?
3. Do you conduct quarterly anti-phishing, smishing and vishing campaigns?[2]
4. Does everyone in your organization understand the risk associated with cybersecurity, the common ploys used by threat actors and how to report any suspicious activities for further investigation?

Access Control
5. Are all vendor default accounts changed or disabled?
6. Are only necessary services, protocols, daemons[3] and functions enabled?
7. Is all unnecessary functionality removed or disabled?
8. Are all accounts immediately disabled or deleted upon termination of employment?
9. Are all screen idle times set for 15 minutes, and do they require reauthentication to unlock?

End User
10. Do you provide end users a tool to save all passwords (preferably cloud-

based for home and work use)?
11. Have you developed an administrator (admin) and user password or passphrase policy that eliminates the use of common or easy-to-guess passwords?

End Points

12. Are all end point logs being ingested by a smart technology that uses threat intelligence and artificial intelligence (AI) based on threat actor activities and heuristics?
13. Do you harden all endpoints and remove everything that is not needed for job functionality?
14. Do you have next generation anti-malware protection (e.g., managed detection and response [MDR], extended detection and response [XDR], endpoint detection and response [EDR])[4] on all endpoints that utilizes a threat intelligence-based security analytics platform with built-in security context?
15. Do you prevent nonenterprise-controlled and secured devices from connecting to any portion of your network?
16. Do all end points have personal firewalls for accessing the Internet when not attached to the enterprise network?
17. Do all end points have antivirus software installed that cannot be disabled and is automatically updated when new updates are available?
18. Do all end points have a next generation anti-malware application installed?

Event Management

19. Are all logs stored for at least 2 years?
20. Are all devices generating logs?
21. Are all logs being reviewed daily by inside and/or outside sources?
22. Do you have a mature and well-organized cybersecurity incident response (in-house or in conjunction with third parties) that thoroughly investigates all incidents?

Security Architecture

23. Do you only give employees the tools and access needed to perform their job functions, and nothing else?
24. Do you utilize the principle of least privilege?
25. Do you deploy a zero trust model?
26. Do you require multifactor authentication (MFA) for all connections outside of the network?
27. Do you require MFA for internal authenticated network users to access key infrastructure and data inside the network (i.e., the crown jewels)?
28. Do you manage all credentials in an order that allows you to quickly conduct a password reset for every account on your network? (This includes service accounts.)
29. Have you recently assessed your Active Directory to ensure that it is properly configured and secured?
30. Are you actively monitoring the security of your Active Directory?

31. Do your perimeter firewalls have a deny-all rule unless otherwise authorized?
32. Is your demilitarized zone (DMZ) secured?
33. Has it been ensured that there are no data, databases or stored accounts on the DMZ?
34. Do you deploy anti-spoofing technology to prevent forged IP addresses from entering the network?
35. Do you prevent the disclosure of internal IP address and routing information on the Internet?
36. Do you segment key infrastructure from other parts of the network with restrictive firewalls (e.g., segmenting WiFi, confidential data, virtual machines and printers away from crown jewels)?

Cryptography
37. Are procedures defined and implemented to protect cryptographic keys used to protect stored data against disclosure and misuse?
38. Are cryptographic keys stored in the fewest possible locations with at least dual custodians?
39. Do you utilize full disk encryption on all appropriate drives?
40. Do you use secure encryption in motion—at least Transport Layer Security (TLS) 1.1 or higher?
41. Is all nonconsole administrative access encrypted using strong cryptography?

Threats
42. Do you perform periodic targeted threat hunts?
43. Do you ingest current threat intelligence (preferably from more than one source) and have a procedure to implement rapid countermeasures based on good threat intelligence?
44. Does it include performing routine dark web reconnaissance to learn what exists on the dark web about your brand and enterprise structures?
45. Do you closely monitor all vendor and third-party supply-chain connections for compliance and untoward issues?

Testing
46. Do you conduct at least 1 penetration test annually, performed by a third party?
47. Do you conduct routine vulnerability scans and remediate all vulnerabilities with a Common Vulnerability Scoring System (CVSS) score of 4 or more within 30 days, and all other vulnerabilities within 90 days?
48. Do you routinely scan your Internet-facing infrastructure for penetration and vulnerabilities?
49. Do you perform an annual business impact analysis/risk analysis report with insider and outside auditors?

Policy
50. Do you have an enterprise security policy that is updated at least annually

and understood by all parties to which it applies?
51. Do you have a formal change control policy?

Physical

52. Are processes and mechanisms for restricting physical access to servers, consoles, backup and network equipment in place and properly safeguarded?
53. Are physical and/or logical controls implemented to restrict the use of publicly accessible network jacks within the facilities?

Plans

54. Do you have a good cyberincident response plan (CIRP) that is reviewed and practiced yearly? The CIRP should be routinely updated, and the core and extended incident response teams should practice responses at least annually using tabletop or functional cybersecurity exercises.
55. Do you have playbooks with technical instructions for handling common cybersecurity incidents?

Inventory

56. Do you have thorough diagrams of the entire network, including WiFi?
57. Do you have a complete inventory of all assets that includes business criticality levels, owners, co-owners and restoration? Does this inventory include instructions with time periods to recover?
58. Do you have a full set of data flow diagrams?

Data Management

59. Do you utilize file integrity monitoring (FIM) of the crown jewels of the organization?
60. Is storage of confidential data kept to a minimum and securely deleted after it’s no longer needed?
61. Do you require data classification throughout the network?
62. Do you deploy a network and cloud-based data loss prevention (DLP) program anywhere confidential data reside?
63. Do you prevent confidential data from being copied to external devices and external devices from being attached to end points?

Software Development

64. Are processes and mechanisms for developing and maintaining secure systems and software defined and understood?
65. Are software engineering techniques or other methods defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in all software?
66. With regard to public-facing web applications, are new threats and vulnerabilities addressed on an ongoing basis?
67. Are these applications protected against attacks?
68. Are preproduction environments separated from production environments, and is separation enforced with access controls?

Mobile Devices
69. Are all mobile devices governed by effective mobile device management (MDM) policies?
70. Do you disallow any connectivity of mobile devices not controlled by enterprise security mechanisms?

Conclusion

So, did you find entropy? Did you find additional layers of protection that could be included with a defense in depth (DiD)[5] cybersecurity strategy? Remember, your answers to these questions reflect merely a single point in time. Things change with time—entropy occurs. Technologies change, strategies change, and threat actors continue to make progress and hone their skills.

It is also worth remembering that while each of the items on the list reduces risk, even if you can confidently answer affirmatively to all 70, you have not eliminated all risk. If there are items that have not been addressed, they are likely worth adding to your cybersecurity road map as soon as possible.

Endnotes

[1] OpenStax, "12.3 Second Law of Thermodynamics: Entropy," *Physics*
[2] Center for Internet Security (CIS), "Vishing and Smishing: What You Need to Know," February 2023
[3] Brans, P.; "Daemon," *TechTarget*
[4] Hayes, N.; "EDR vs. MDR vs. XDR," CrowdStrike, 18 April 2023
[5] Center for Internet Security, "Election Security Spotlight—Defense in Depth (DiD)"