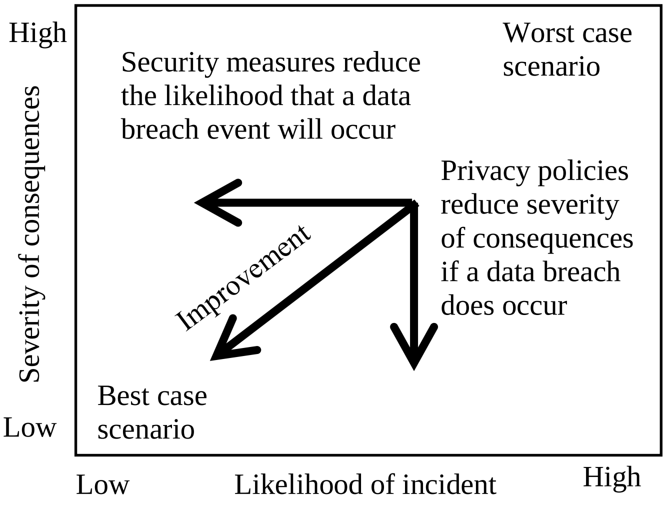
Cybersecurity Checklist

Here is a list of suggestions to help reduce your risk of a data breach. It's not comprehensive; certainly other items could be added. However, most organizations probably aren't doing all of the things they should, so it is likely you'll find something here to improve.

Spread the word – share this with others who may need it

1. Perform timely, properly-focused and scoped risk assessments
2. Have well-defined, security-minded policies & procedures documented that address the risks identified in risk assessments
3. Train employees and others (vendors, contractors, …)
   a. Policies & procedures
   b. Risk and threat awareness (so they can identify new risks and threats on their own)
4. Manage third party risks
   a. Contract for minimum requirements (best practices)
   b. Contract right to audit and test
   c. Actually perform audits and testing
   d. Consider requiring cyber/privacy incident insurance
5. Test on the training, to ensure it is effective and being followed
   a. Everyone who merits training
   b. Include third parties, even if they are not included within your own training
   c. Example: phishing tests
6. Have a risk management plan (RMP) in place that addresses risks identified in your risk assessments
7. Have an incident response plan in place that addresses risks identified in risk assessments, and lays out solid plans for rapid recovery from all categories of risk (more than just cyber risks)
   a. Include business continuity planning (fire, flood, others)
   b. Have service providers lined up, contract terms agreed upon, including work items and prices, if possible
8. Perform table top exercises to test your risk management plans
9. Perform audits of incident response plans, regularly
   a. Test all plans and update all relevant documents
   b. Use internal audits to prepare for external audits
   c. Then use the external, independent auditors
10. Use penetration testers ("white hat hackers")
   a. Focused (initially) on specific vulnerabilities, later …
   b. Open ended tests for discovering new weaknesses
11. Require use of multi-factor authentication for login accounts
12. Require use of a secure password manager
   a. Explicitly stated requirement in your policies & procedures
   b. Prohibit storing access credential information, such as lists of usernames and passwords, on networked computers
13. Proactively manage all login-access account authorizations
   a. Require all accounts to be locked/frozen/deleted/modified within a short time after employee or contract termination
   b. Regularly audit whether all credentials are currently authorized (i.e., ensure no ghost accounts)
   c. Both email and resource user accounts
14. Prevent shadow access of authorized users
   a. Block multiple simultaneous logins from different devices, wherever practical
   b. Force audits of email rules (prohibit automatic bcc or forwarding, or diversion of incoming emails into the user's deleted items folder)
15. Ensure network protections tools are installed, operating and fully up-to-date
   a. Anti-virus
   b. Firewalls
   c. Filters
   d. Malware detection & removal
16. Have an intrusion detection system in place and operating
   a. Keep activity logs for longer than the likely long-term undetected advanced persistent threat (APT)
17. Automatically scan emails
   a. For malware
   b. For intellectual property (IP) leakage, such as trade secret keywords
   c. Both incoming & outgoing emails
18. Use the least privilege necessary for performing functions
   a. Limit administrator rights to specified information technology (IT) staff
   b. Prohibit most employees from installing software
   c. Do not surf the internet with an administrator account
19. Disable all non-critical remote access
20. Encrypt data
   a. Stored data at rest
   b. In transit, if possible
   c. Proper key management is critical
21. Segment your network with differing access credentials by legitimate data access needs
22. Air gap data whenever practical
   a. Your ***crown jewels***
   b. Highly sensitive data
   c. Data presenting severe liability risk
   d. Encryption keys that are not in active use
23. Limit software installation to only programs known to be safe
   a. Consider whitelist-only, with integrity-verified copies
   b. Blacklist dangerous programs, such as file-sharing software
24. Ensure that security updates and patches are kept current
   a. Follow up with audits to ensure that patches are actually applied in a timely manner
   b. Ensure patches are legitimate, rather than malware
   c. Applications (apps) and operating system (OS)
25. Remove outdated or unsupported software
   a. If legacy data requires specific outdated software to access, keep re-installation copies of the software off-line
26. Backups should be
   a. Done on timely intervals (regularly, plus after activities that generate important data, and also prior to system changes)
   b. Stored off-line
   c. Stored off-site
   d. Segmented by data type and date
   e. Redundant
   f. Sufficiently far back in time to pre-date long-term, undiscovered advanced persistent threats (APTs)
   g. Encrypted – ***with keys stored separately***
27. Test backups with restoration dry-runs

Privacy ≠ Security | *You need BOTH!*


High
Low
Severity of consequences
Security measures reduce the likelihood that a data breach event will occur
Worst case scenario
Privacy policies reduce severity of consequences if a data breach does occur
Improvement
Best case scenario
Low
Likelihood of incident
High

Provided by **Kelce S. Wilson**, PhD, MBA, JD
CIPP-US | CIPP-E | CIPM | certified privacy professional
Attorney, GrableMartinFulton, PLLC, **972.955.2348**

Cybersecurity Checklist

The human element may be your weakest link

- Since your systems require access by humans to support operations, they can be compromised by error or malice.
- Access points that are needed for you to obtain value from your systems, can be leveraged to become attack points.
- Attackers may try to “piggy-back” legitimate access events rather than “crash the gates”. You need to ensure no “hitchhikers” sneak in.
- Insider threat sources include employees, contractors, vendors & other service providers.

The 3 T’s of securing the human element

1. **T**racking Trust
   a. Beware the malicious insider!
   b. Disgruntled employees, corporate and foreign espionage, …
   c. Background check procedures
   d. Use “Least Privilege” principle
2. **T**ools to Partition and Monitor
   a. Even the most loyal employees need the proper tools
   b. Budget for quality IT needs:
      Back-ups, firewalls, network partitioning, network monitoring tools, end-point security
3. **T**raining & Policies
   a. A careless or untrained employee can create a huge security problem
   b. Even good training can be forgotten
   c. Two basic types:
      1) IT-enforced computer policies
      2) Procedural policies

Suggested 7-step defensive plan

1. Build a security foundation
   a. Best cyber security practices for IT and HR
   b. Take care of the first two T’s for the human element
2. Thorough and effective training & policies
   a. Take care of the third T for the human element
3. Human element active testing
   a. Training is only one-way
   b. To ascertain training effectiveness, you need to test
4. Security-minded data policies
   a. Incident response plan (IRP)
   b. Suggested 3-prong data policy
5. Independent Reviews
   a. Audits and vulnerability assessments
6. White hat penetration tests
7. Ongoing education and re-assessment of security strategy

Details of the suggested 3-prong data policy:

1. Separate
   a. So that a breach does not get everything
   b. Separate by type of information
   c. Separate by privilege (who *really* needs to see what?)
2. Encrypt
3. Purge whatever is not truly necessary

Phase in of the 3-prong data policy:

1. Design a data policy balancing operational needs with risk
2. Implement the new policy for current data collections
3. Then apply policy to on-line, in-use legacy data sets
4. Then apply policy to back-ups and archives

<u>TOP 5 things to do now:</u>

1. Restrict administrator privileges by person and activity
   a. STOP surfing internet with administrator privileges!
   b. For computers (PCs) you own:
      i. Have a user account *without administrator privileges* – this is for normal use
      ii. Have a user account with administrator privileges – *use only for updates and installing **trusted** software*
   c. At the office, only IT staff get administrator privilege
2. Timely procedures: patches, updates, back-ups, network partitioning (firewalls are only part of the solution)
   a. Force timely updates of OS and software applications
3. Strong password management (for important accounts)
   a. 14 or more characters; something you can visualize: Easy solution: adjective + object + action + location
   b. Unique for each account
4. Blacklist risky websites and software
   a. No file-sharing software!
5. Whitelist software installations on critical devices
   a. Restrict installation of executable applications to those that you have a solid basis to trust to be safe

Your IT staff saying “No worries, we’ve got security covered” is NOT the solution.

- Multiple expensive breaches have occurred that were not preventable by best IT practices - More is needed.

For breach prevention efforts (i.e., gap analyses), leverage legal privilege to try preventing use of your own good-faith efforts against you during a lawsuit (e.g., a discovery demand for gap analysis reports), in the unfortunate event of a breach**.**

<u>Privilege cannot be guaranteed!</u>

All you can do is position yourself to argue for it.
   a. The likelihood of success is based on many factors, and can be quite unpredictable
   b. A couple of different types:
      1) Attorney-client communication
      2) Attorney work product
         i. Fact work product
         ii. Opinion work product

One possible argument: The technical and legal risk analyses are so thoroughly interwoven that they are non-separable.

To achieve that, you need a partner who can:

1. Identify legal issues & risks in technical matters
   a. Not all incidents present the same legal risk or reporting and notification obligations
2. Identify technical issues & risks in legal matters
   a. Not all cybersecurity solutions that are advertised by technical consultants will satisfy legal obligations
   b. Efficient preparation involves using technical solutions that fit both real-world security needs and legal obligations, ***simultaneously***
3. Advise you under a plausible claim of legal privilege

Would you hire a patent attorney to draft a patent application who did not understand the technology of your invention?
Would you hire an attorney for your cybersecurity needs who does not understand the technology of hacking?