Things to Remember if Breached

1. **No External Agencies Secured**

- Sometimes a breach is too big to deal with in house.
- Consider contracting with incident response teams when formulating your business continuity / incident response plan.

2. **Enlisting an Outside Attorney is Highly Recommended.**

- No single federal law or regulation governs the security of all types of sensitive personal information.

- As a result, determining which federal law or regulation applies is difficult and complicated.

3. **No Single Decision Maker**

- While there are several parties within an organization that should be on a data breach response team, every team needs a leader.
- There needs to be one person who will drive the response plan, and act as the single source of contact to all external parties.
- They'll also be in charge of controlling the internal reporting structure in order to ensure that everyone, from executives and individual response team members, are kept updated.

4. **No Communications Plan**

- Sticking to the communications theme, another issue organizations face is the lack of planning as it relates to the public, especially the media.

- Companies should have a well-documented and tested communications plan in the event of a breach, which includes draft statements and other materials to activate quickly.

- Failure to ingrate communications into overall planning typically means delayed responses to media and likely more critical coverage

5. **Waiting for the Perfect Information Before Acting**

- Dealing with the aftermath of a data breach often requires operating with incomplete or rapidly changing information, due to new information learned by internal or external security forensics teams.

- Companies need to begin the process of managing a breach once an intrusion is confirmed and start the process of managing the incident early. Waiting for perfect information could ultimately lead to condensed timeframes that make it difficult to meet all of the many notification and other requirements.

6. **Micro Manage the Breach**

- Breach resolution requires team support, and often companies fail when micromanaging occurs.

- Trust your outside counsel and breach resolution vendors, and hold them accountable to execute the incident response plan.

7. **No Remediation Plans Post Incident**

- There should be plans in place that address how to engage with customers and other audiences once the breach is resolved, as well as the establishment of additional measures to prevent future incidents.

- If an organization makes additional investments in processes, people and technology to more effective secure the data, finding ways to share those efforts with stakeholders can help rebuild reputation and trust.

- Many fail to take advantage of this longer-term need once the initial shock of the incident is over.

8. **Not Providing a Remedy to Consumers**

- Customers should be put at the center of decision making following a breach.
- This focus means providing some sort of remedy, including call centers where consumers can voice their concerns and credit monitoring if financial, health or other highly sensitive information is lost.
- Even in incidents that involve less sensitive information, companies should consider other actions or guidance that can be provided to consumers to protect themselves.

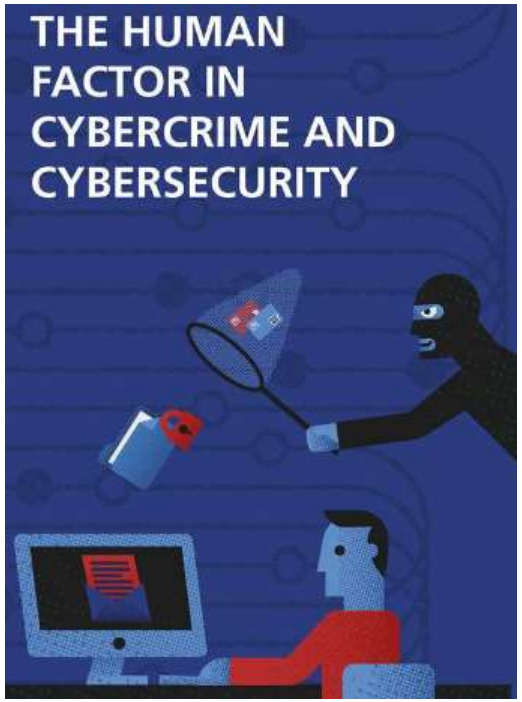
9. **Failing To Practice**

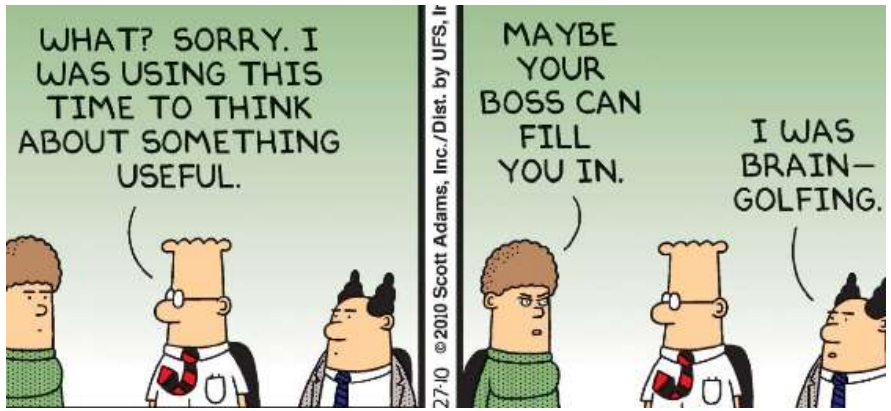
- Above all, a plan needs to be practiced with the full team.
- An incident response plan is a living, breathing document that needs to be continually updated and revised.
- By conducting a tabletop exercise on a regular basis, teams can work out any hiccups before it's too late.

Conclusion:

No matter how secure your application is, it is always vulnerable to "The Human Factor".

This human factor is the weakest link in security which can be patched not by one time training but only by an ongoing process of improvement.





Many times it's rather the interaction between the data and the person has to be secured rather than the interaction between data and server.