

5 KEY TAKEAWAYS

Government Contractors: Best Practices & Prevention Strategies for Data Breaches

Kilpatrick Townsend's [Gunjan Talati](#) and [Chris Henel](#), members of the firm's Government Contracting Team, recently presented a webinar in collaboration with Federal Publications' Cybersecurity Institute on best practices and prevention strategies for government contractors when dealing with data breaches. Data breaches can be costly and chaotic but there are a few things contractors can do to prepare.

5 key takeaways from the discussion include:

1

As IT systems modernize and cyber-criminals become more sophisticated, the risk of a cybersecurity breach affecting the integrity, confidentiality and availability has become harder to detect and thwart.

Government agencies recognize that its data, contractors' data, and the personally identifiable information (PII) of U.S. citizens are all at risk more than ever before and the Government is seeking to place the burden of safeguarding this data on contractors as much as possible.

2

3

Contractors can develop compliant and secure information systems by establishing a culture of compliance that sets a tone at the top and promotes safe system use and the safe storage and transmission of data at all levels of the company.

Having a written, well-defined system security plan and incident response plan can save a Government contractor from a "cyber-catastrophe" and protect the Government and U.S. citizens in the process. Implement testing, training and exercises to ensure that the plan works as it should when a cyber-event occurs.

4

5

Advances in artificial intelligence and machine learning technology can assist Contractors in being proactive about cyber-events as opposed to reactive.

For more information, please contact:

Gunjan Talati at gtalati@kilpatricktownsend.com or Chris Henel at chenel@kilpatricktownsend.com

www.kilpatricktownsend.com