



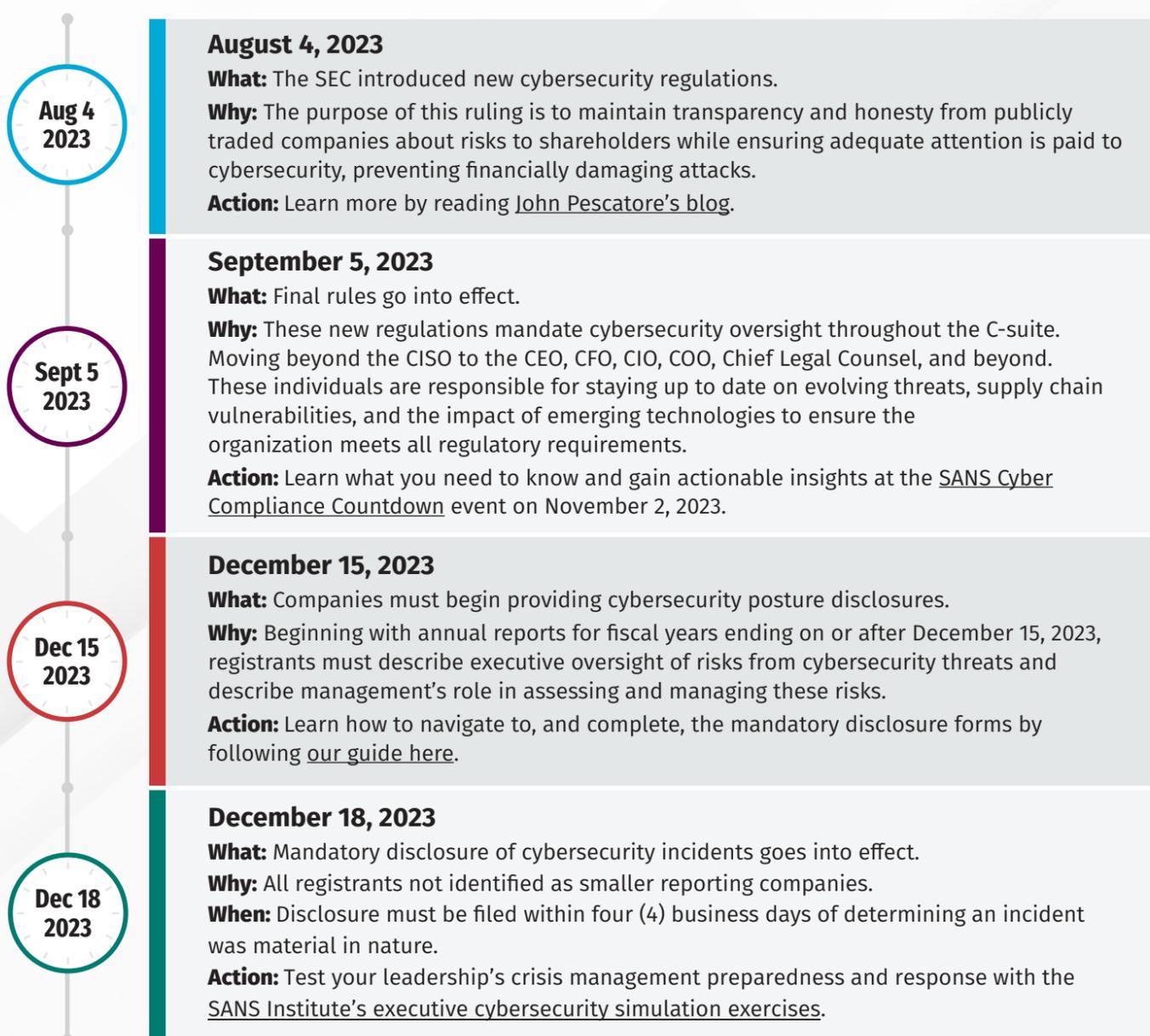
Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

A Rule by the Securities and Exchange Commission

Earlier this year, the Securities and Exchange Commission (SEC) published the final rules in the Federal Register on cybersecurity risk management, strategy, governance, and incident disclosure.

What Does This Mean?

- Publicly traded companies registered with the SEC and bound by the Securities Exchange Act of 1934 reporting requirements must adhere to this new amendment.
- After a cybersecurity incident has been deemed to be a material incident, the company must comply with required disclosure requirements.
- As of the time of publication, the SEC has stated that a materiality determination of the cybersecurity must be made without unreasonable delay.
- Consult our easy-to-follow timeline below to help your organization prepare effectively for the new compliance rules.



Conclusion

These updated SEC cybersecurity requirements highlight the importance of establishing a comprehensive security culture within your organization. This culture should encompass both cyber practitioners and all levels of management. Information sharing, effective IT governance, and consistent training for both technical experts and managerial personnel are essential.

