NEW SEC REGULATION

TAKING THE DATA CENTRIC APPROACH

U04

galaxkey®
www.galaxkey.com

PROTECT YOUR DATA

Share files with confidence

Communicate securely

Protect all your data

A cybersecurity breach is a material breach

The Securities and Exchange Act of 1934 was created by the Securities and Exchange Commission (SEC). It ensures transparency and fairness in the capital markets. In **2011**, the agency clarified that significant cybersecurity-related risks and incidents need to be disclosed. There was another update in **2018** that cited the "ongoing risks and threats to our capital markets" from cybersecurity incidents.

In **July 2023**, SEC made it clear that a cyber breach is a material breach and companies *must* disclose it.

Supply chain disruptions, like semiconductor shortages and natural disasters, can harm a company's finances and stock value. Similarly, cybersecurity breaches are a big threat. They lead to immediate costs to stop the attack, loss of customers and revenue, and possible lawsuits from shareholders and customers. The company's insurance premiums might go up, and auditors and the board of directors will scrutinize it more. Cybersecurity incidents also distract management from other tasks and make customers question the company's security. This might lead to hiring lawyers and experts, increasing costs.

Any business that depends on a digital infrastructure now needs to consider that a cybersecurity breach is considered a material breach.

$1 million settlement: Pearson PLC

In 2021, British publishing company Pearson PLC paid $1 million to settle charges that it misled investors following a data breach and theft of millions of student records.

$500,000 settlement: First American Financial Corp

First American Financial Corp settled a charge of $500,000 fine for lack of disclosure controls following the discovery of a vulnerability in its system. That vulnerability exposed 800 million image files, including Social Security numbers and financial information.

A DATA BREACH IS A MATERIAL BREACH

U04

What does the SEC 2023 Regulation say?

Material Cybersecurity incidents
If a company has a cyber breach, the company must disclose the breach within 4 working days by filing the Form 8-K.

Cybersecurity Risk Management & Strategy Disclosures
Under the newly adopted Regulation S-K Item 106 in a registrant's Form 10-K, registrants must describe their processes for the "assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition."

Governance and Board Oversight Disclosures
Registrants must describe the board's oversight of risks from cybersecurity threats as well as management's role in assessing and managing material risks from cybersecurity threats and, if applicable, "identify any board committee or subcommittee responsible" for such oversight "and describe the processes by which the board or such committee is informed about such risks," under Item 106(c) in a registrant's Form 10-K.

Protecting data is a must to reduce the material breach

Cybersecurity breach is in two forms:

- Network centric
- Data centric

In both forms, the threat actor wants to steal digital data. The quantum of data equates to the value of the breach.

In the last 20 years, we've learned that relying solely on a network-centric approach isn't reliable. Network defenses get breached frequently.. To reduce the impact of a cybersecurity breach, you must protect your data even if the network is breached.

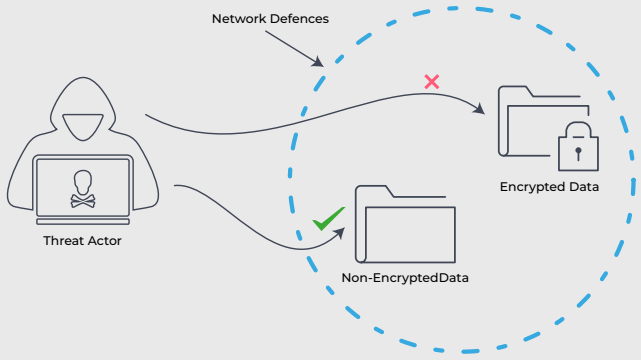
Imagine a scenario: a company faces a cybersecurity breach, and a lot of data is stolen by malicious actors. If the stolen data is useless to them, the impact of the breach is greatly reduced. This highlights the importance of having a robust data protection system in place.

Companies must shift their perspective on data protection. **It needs to be separate from networks, devices, and applications**. This is the only way to prevent bad actors from accessing data, which would be a significant breach.

Data Encryption

To keep data safe, encryption is the key. If a bad actor breaches network defenses, they can access unprotected data, but even if they get to encrypted data, it's worthless to them.

By using good data encryption, companies can minimize the impact of material breaches because it reduces the losses. Also, companies can show they've taken the right steps to protect data effectively.



galaxkey®
www.galaxkey.com

SEC REGULATIONS CREATE A DOMINO EFFECT

U04

Do SEC regulations affect your company?

SEC rules apply to all public listed companies. If you're a public company or you're a part of a supply chain, these rules will impact you in some way. Nowadays, business relies on digital data, so just as paper records were protected, digital data also needs to be safeguarded.

Data can be breached either in transmission or in store. Hence it is required that companies look into protecting data in at least the following use cases

- Exchanging sensitive emails which is the primary communication medium
- Sharing and receiving large files using managed file transfer
- e-Signatures where businesses have to sign documents which contain sensitive data
- File archiving where companies store historical data
- Instance messaging which is the new medium of communication

In all use cases, data needs to be protected and be accessible only for the intended recipient.

When public listed companies work with both listed and non-listed firms, they must protect their data. SEC regulations affect everyone involved, creating a ripple effect.

Network breaches happen when bad actors obtain information that helps them attack networks. This underscores the importance of data protection.

The Cloud

Companies are shifting to the cloud and entrusting their sensitive data to third-party providers. They depend on these providers to keep their data safe. Lately, there have been attacks on these providers, resulting in companies' data being compromised. Therefore, companies must take a proactive approach to secure their data, even when it's stored with third parties. This is especially important for companies subject to SEC regulations.

How can we help?

Galaxkey is an encryption platform that works separately from networks, devices, and applications. We have products based on Galaxkey tech to address different business needs. Reach out to us, and our team can guide you and offer the right solution to help your business comply with SEC regulations.

Contact us today for a demo.

Email: sales@galaxkey.com