SideChannel

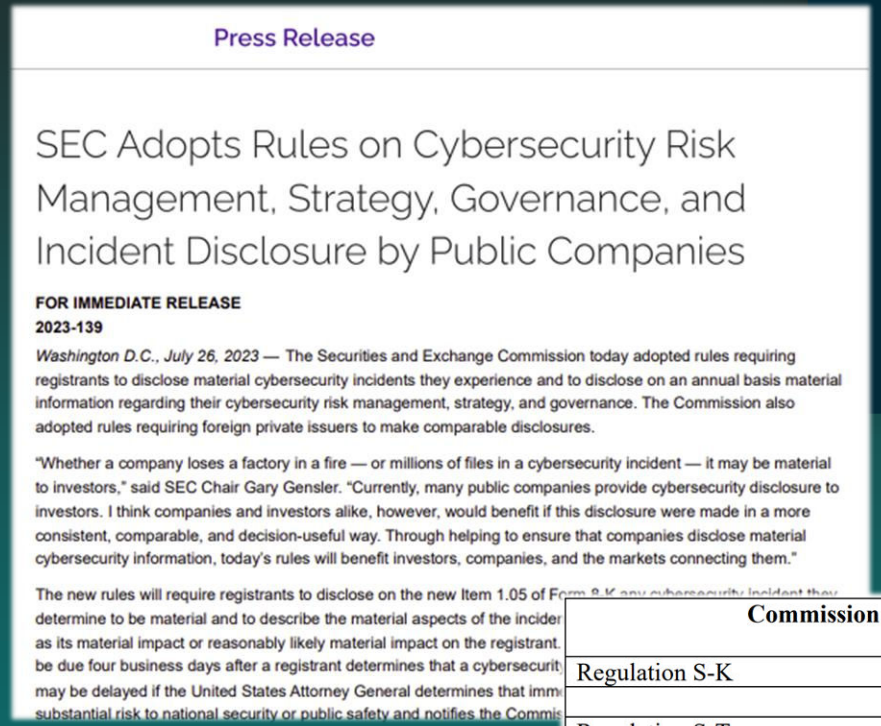
SEC Cyber Program

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Final Rule

Effective September 5th, 2023

The Securities and Exchange Commission adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance.



Press Release

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

FOR IMMEDIATE RELEASE
2023-139

Washington D.C., July 26, 2023 — The Securities and Exchange Commission today adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The Commission also adopted rules requiring foreign private issuers to make comparable disclosures.

"Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors," said SEC Chair Gary Gensler. "Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them."

The new rules will require registrants to disclose on the new Item 1.05 of Form 8-K any cybersecurity incident they determine to be material and to describe the material aspects of the incide
as its material impact or reasonably likely material impact on the registrant.
be due four business days after a registrant determines that a cybersecurit
may be delayed if the United States Attorney General determines that imm
substantial risk to national security or public safety and notifies the Commis

Commission Reference		CFR Citation (17 CFR)
Regulation S-K		§§ 229.10 through 229.1305
	Items 106 and 601	§§ 229.106 and 229.601
Regulation S-T		§§ 232.10 through 232.903
	Rule 405	§ 232.405
Securities Act of 1933 ("Securities Act")[1]	Form S-3	§ 239.13
Securities Exchange Act of 1934 ("Exchange Act")[2]	Rule 13a-11	§ 240.13a-11
	Rule 15d-11	§ 240.15d-11
	Form 20-F	§ 249.220f
	Form 6-K	§ 249.306
	Form 8-K	§ 249.308
	Form 10-K	§ 249.310

Complete Delivery

SideChannel delivers a robust cybersecurity strategic plan & operational program with an experienced team of CISOs, engineers, and project management to build, execute, and govern any cybersecurity policies, implemented solutions, and 3rd party providers.

Processes Matured	**Policies Documented**	**Program Led & Governed**
Engineering Staffed	**Projects Completed**	**Solutions Implemented & Managed**

Phase I Solutions

Small Companies (Revenues < $100M)
$30,000 Annual Retainer

Large Companies (Revenues > $100M)
$50,000 Annual Retainer

Supports SEC requirements except Item 106(2)(ii)

Baseline Cyber Program to Meet Requirements

Risk Management

1. Cyber risk assessment and quarterly reporting
2. Standard / control gap analysis (*against SEC noted "NIST CSF"*)
3. 18-month strategic cybersecurity roadmap
4. Documentation on cybersecurity risk management as part of business operations

Personnel

1. Annual retainment of SideChannel cybersecurity service provider
2. Qualified dedicated vCISO with documented and checked resume
3. Company cybersecurity program with governance, policy & process
4. Third party risk management (TPRM) program

Documentation

1. Written information security policy
2. Written incident response plan (IRP)
3. Table-top exercise (TTX)
4. Breach Assessment and Reporting Service (BARS)
5. Incident after action review (AAR) & root cause analysis (RCA)
6. On-prem & SaaS asset inventory

Board Support

1. Board cyber program agenda, documented committee structure
2. Board reporting by vCISO

Phase II Solutions

Budget Based on Organization Size

Calculated by # of Employees & IT Infrastructure

Supports Item 106(2)(ii)

*The processes by which such persons or committees are informed about and monitor the **prevention, detection, mitigation, and remediation** of cybersecurity incidents.*

Deployable Technologies (Managed or Unmanaged Service)

Prevent

- Zero Trust (Microsegmentation)
- Vulnerability Management
- Email Security
- User Training
- Multi-Factor Authentication (MFA)

Detect & Mitigate

- Identity Detection & Response
- Endpoint Detection & Response
- Web, application and/or network penetration tests

Remediate

- Engineering Services
- Project Management and Implementations

Solution Mapping to SEC Final Rule

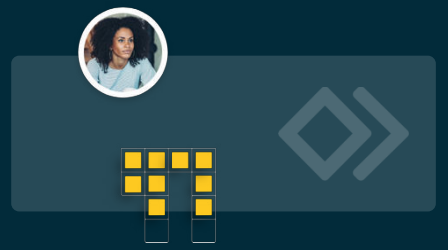
SEC Rule	SideChannel Solution
Item 1.05	Written incident response plan (IRP), 1 table-top exercise (TTX), Breach Assessment and Reporting Service (BARS)
Item 106(b)(1)	Risk assessment, control gap analysis, 18-month strategic roadmap, information security policy, written incident response plan (IRP), user training
Item 106(b)(1)(i)	Documentation on cybersecurity risk management as part of business operations
Item 106(b)(1)(ii)	Retainment of SideChannel as vCISO and cybersecurity service provider
Item 106(b)(1)(iii)	Third party risk management (TPRM) program and documentation
Item 106(b)(2)	Incident after action review (AAR), root cause analysis (RCA)
Item 106(c)(1)	Board cyber program agenda, documented committee structure, and reporting templates
Item 106(c)(2)	Cybersecurity program with governance, policy & process
Item 106(c)(2)(i)	Qualified vCISO on retainer with documented and checked resume
Item 106(c)(2)(ii)	Cyber program aligned to a standard (*NIST CSF preferable – Protect, Detect, Respond, Recover*), risk assessment reporting, technology implementations, penetration testing
Item 106(c)(2)(iii)	Board reporting templates, agenda, and minutes

Making cybersecurity simple and accessible

info@sidechannel.com

Appendix – Use cases

Success Stories
Public Companies



Riot Platforms, Inc.

RIOT Market Cap $2.44B

CRISPR Therapeutics AG

CRSP Market Cap $3.84B

BlackBerry Limited

BB Market Cap $2.6B

Shift Technologies, Inc.

SFT Market Cap $23.57M

Embark Technology, Inc. (acquired, delisted)

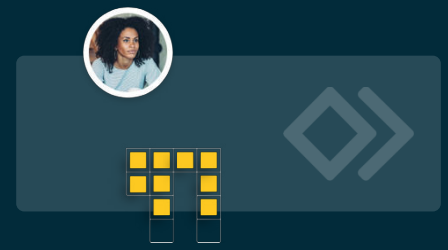
EMBK Market Cap $70.2M

SideChannel, Inc.

SDCH Market Cap $15M

Success Stories

Startups



FinTech - High speed trading platform (including crypto currency)

Built and managed the cyber program from the ground up from due diligence, Seed Round, to $40m Series A, and then to the Citi Group led $100m Series B

Healthcare SaaS – SaaS electronic health record

Instrumental in maturing the cyber program to enable the Co. to win the pilot for what could be their single largest customer. Critical in post-merger integration efforts of 4 new entities to the enterprise.

AI/ML Technology – SaaS note-taking and AI/ML transcription

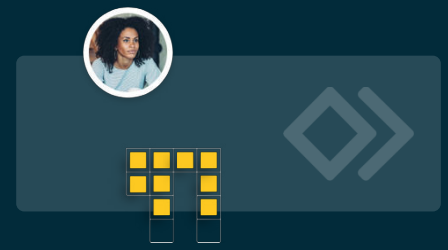
Pivotal sales enablement through third-party risk management support, including customer facing meeting, negotiations, and remediation.

Autonomous Vehicles – Autonomous commercial vehicle startup

Combined assessments of enterprise security and technology platform for a recent unicorn, post IPO as the initial starting pointfor a holistic enterprise security program.

Success Stories

Mid-Market



Crypto Currency Operations –
One of the largest N. American bitcoin mining operations

Comprehensive information security program development and post-merger integration for this publicly traded bitcoin Company.

Sporting Goods Manufacturer –
ecommerce / brick-and mortar retail

Information Security and IT Program development, implementing key cyber technologies, policies, procedures and managed IT services.

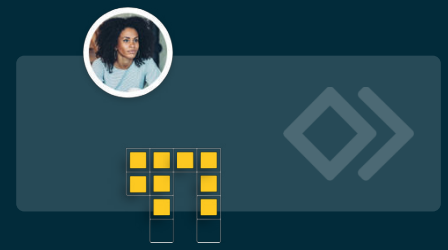
SaaS HR Mgmt –
Cloud based performance management provider

Information Security Program leadership to mature this SaaS provider's security profile, which is the winner G2 2022 Best Software Award.

International IT Services Co. –
A Canadian publicly traded IT Services Provider

Interim CISO services and transition to new full-time CISO and ongoing CISO Advisory Services.

Success Stories
Enterprises



Maritime – Premier International Cruise Line

Information Security and Privacy Program development. Combined expertise supporting this global Co. With vCISO and vCPO services.

Global Industrial Manufacturing

CMMC evaluation and compliance. Modernized outdated security technology controls with global, efficient, technology and services

Biotech/Life Sciences – Leading gene editing life sciences biotech

Comprehensive cyber security leadership and operational support for this cutting-edge biotech.

Biomedical Research Institute (non-profit)

Information Security and IT Program development, establishing key technologies, policies and procedures. Established support with both managed IT and managed Incident Response services.